

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO
Departamento de Engenharia Electrotécnica e de Computadores

Planeamento de uma Rede de Comunicações para o Instituto Superior de Ciências da Educação do Lubango, Angola

Yola Filomena Ferreira Marinheiro Lima



Universidade do Porto
Faculdade de Engenharia
FEUP

Dissertação submetida para a obtenção do grau de
Mestre em Engenharia Electrotécnica e de Computadores

Dissertação realizada sob a supervisão dos Professores Manuel Alberto Pereira
Ricardo e João Manuel Couto das Neves

Porto, Setembro de 2009

Planeamento de uma Rede de Comunicações para
o Instituto Superior de Ciências da Educação do
Lubango, Angola

Yola Filomena Ferreira Marinheiro Lima

Orientador: Professor Manuel Alberto Pereira Ricardo

Co-Orientador: Professor João Manuel Couto das Neves

*À meu Marido
e à minha Filhinha*

Resumo

A educação é decisiva e fundamental para proporcionar e assegurar o desenvolvimento sócio-económico de um País. Com isso, torna-se necessário preparar todos os elementos envolvidos no processo ensino-aprendizagem, para levar a bom termo tal desafiadora tarefa.

Um campus universitário necessita de possuir tecnologias de comunicação que permitam partilhar a informação existente num conjunto de sistemas ligados entre si, de forma a proporcionar uma melhor experiência de aprendizagem. A este conjunto de sistemas dá-se genericamente o nome de rede. Numa rede todos os seus elementos, como por exemplo os computadores, estão ligados entre si de modo a poderem partilhar recursos, dados e programas.

Este projecto tem como objectivo o estudo e o planeamento da rede de comunicações para o Instituto Superior de Ciências da Educação em Angola, de modo a proporcionar a esta instituição uma melhor qualidade de ensino e facilitar a organização administrativa da mesma. Com este projecto pretendeu-se também antecipar e permitir futuras mudanças da rede de forma a possibilitar o seu crescimento.

Palavras-Chave: Planeamento, Rede local, Fluxos, Internet

Abstract

Education is decisive and fundamental to ensure the social and economic development of a country. Thereby, it becomes necessary to prepare every element involved in the teaching-learning process.

Nowadays, in a university campus, there is a need of communication technologies, used the exchange information between a set of interconnected systems. This set of systems can be generically named as network. In a network devices, such as computers are interconnected in a way that allows them to share resources, data and programs.

The objective of this project is to study and plan a communications network for the Instituto Superior de Ciências da Educação in Angola, in order to provide this institution with a better teaching quality and ease its administrative organization. It was also intended with this project to predict future changes to the network, in order to also enable its growth.

Keywords: Planning, Local Network, Flows, Internet

Agradecimentos

Quero agradecer em primeiro lugar ao meu Marido António Lima, que me deu força e incentivo para fazer o mestrado.

Muitas pessoas contribuíram para o desenvolvimento deste projecto; professores e um colega. Gostaria de agradecer muito em especial ao Professor Manuel Ricardo por todo o seu apoio.

Gostaria de agradecer também ao Professor João Neves, por sua paciência e ajuda de modo a levar esta tese para sua conclusão.

Os meus agradecimentos também ao meu colega e amigo Luís Lemos, que nunca se recusou a dar-me o seu apoio sempre que este lhe foi requisitado.

Gostaria de agradecer, as lindas e adoráveis senhoras do Departamento de Engenharia Electrotécnica e de Computadores, Rosário Rebelo e a Susana Dias, pelo apoio, convivência e amizade que sempre depositaram em mim.

Abreviaturas

ABR	⇒ Available Bit Rate
AD	⇒ Adaptativas
ADSL	⇒ Asymmetric Digital Subscriber Line
AP	⇒ Access Point
AS	⇒ Autonomous System
BE	⇒ Best-effort
BGP	⇒ Border Gateway Protocol
CBR	⇒ Constant Bit Rate
CDN	⇒ Content Delivery Network
CHAP	⇒ Challenge Handshake Authentication Protocol
CM	⇒ Continuous-media
CSMA/CD	⇒ Carrier Sense Multiple Access with Collision Detection
DDR	⇒ Dial on Demand Routing
DIN	⇒ Deutsche Institute fur Normung
DHCP	⇒ Dynamic Host Configuration Protocol
DNS	⇒ Domain Name System
EIA	⇒ Electrical Industries Association
EGP	⇒ Exterior Gateway Protocol
FTP	⇒ File Transfer Protocol
HTTP	⇒ Hypertext Transfer Protocol
IEC	⇒ International Electrotechnical Commission
IEEE	⇒ Institute of Electrical and Electronics Engineers
IGP	⇒ Interior Gateway Protocol
IMAP	⇒ Internet Message Access Protocol
IP	⇒ Internet Protocol
IPSec	⇒ IP Security

ISCED	⇒ Instituto Superior de Ciências da Educação
ISO	⇒ International Organizatio for Standardization
ISP	⇒ Internet Service Provider
ITU-T	⇒ International Telecommunication Union -Telecommunication Standardization
LAN	⇒ Local Area Network
MAC	⇒ Media Access Control
MIB	⇒ Management Information Base
NAT	⇒ Network Address Translation
OSPF	⇒ Open Shortest Path First
PAP	⇒ Password Authentication Protocol
PAT	⇒ Port Address Translation
PC	⇒ Personal Computer
POP	⇒ Post Office Protocol
PPP	⇒ Point-to-Point Protocol
QoS	⇒ Quality of Service
RADIUS	⇒ Remote Authentication Dial-In User Service
RIP	⇒ Routing Information Protocol
RMON	⇒ Remote Monitoring
SMTP	⇒ Simple Mail Transfer Protocol
SNMP	⇒ Simple Network Management Protocol
STP	⇒ Spanning Tree Protocol
TCP	⇒ Transmission Control Protocol
TIC	⇒ Tecnologias de Informação e Comunicação
UBR	⇒ Unspecified Bit Rate
UDP	⇒ User Datagram Protocol
UPS	⇒ Uninterrupted Power Supply
VBR	⇒ Variable Bit Rate
VCoIP	⇒ VideoConference over IP

VLAN	⇒ Virtual LAN
VoIP	⇒ Voice over IP
WAN	⇒ Wide Area Network
WMN	⇒ Wireless Mesh Networks
WWW	⇒ World Wide Web

Índice Geral

Resumo	5
Abstract.....	6
Agradecimentos	7
Abreviaturas.....	8
Índice Geral	11
Índice das Figuras	14
Índice das Tabelas	16
Índice das Fórmulas.....	17
1 Introdução	18
1.1 Objectivos e Metodologia.....	21
1.2 Resultados do Projecto.....	22
1.3 Estrutura do Relatório	23
2 Estado da Arte	25
2.1 Análise de Requisitos.....	25
2.1.1 Utilizador.....	25
2.1.2 Aplicações e Serviços	26
2.1.3 Dispositivos.....	29
2.1.4 Rede.....	30
2.1.4.1 Arquitectura.....	36
2.1.4.2 Hierarquia.....	40
2.1.4.3 Endereçamento	41
2.1.4.4 VLAN	42
2.1.5 QoS.....	43
2.1.5.1 Débito	44
2.1.5.2 Atraso	45
2.1.5.3 Perdas ou Taxa de Erros.....	46

2.2	Análise de Fluxos.....	47
2.2.1	Tipos de Fluxos	50
2.2.1.1	Fluxos Individuais	50
2.2.1.2	Fluxos Agregados.....	51
2.2.2	Modelos de Fluxos	52
2.2.3	QoS dos Fluxos Individuais	55
2.2.3.1	Caracterização do Débito	55
2.2.3.2	Caracterização do Atraso.....	57
2.2.3.3	Caracterização das Perdas	58
2.2.4	Técnicas dos Fluxos Agregados.....	58
2.2.5	Medições de Fluxos.....	59
2.3	Equipamentos de Rede.....	60
2.4	Resumo.....	62
3	Projecto da Rede	63
3.1	Levantamento de Requisitos	63
3.1.1	Utilizador.....	63
3.1.2	Aplicações	65
3.1.3	Dispositivos.....	69
3.1.4	Rede.....	70
3.1.4.1	Definição dos Locais a Abranger pela Rede	71
3.1.4.2	Definição da Topologia da Rede	72
3.1.4.3	Redundância	73
3.1.4.4	Definição dos Locais das Aplicações por Edifício.....	74
3.1.4.5	Restrições da rede.....	78
3.2	Topologia do ISCED.....	79
3.3	Dimensionamento	81
3.3.1	Especificação dos Fluxos	82
3.3.2	Ligações	86
3.4	Arquitectura Lógica da Rede	87

3.4.1	VLAN.....	92
3.5	Especificações dos Equipamentos	94
3.5.1	Cablagem.....	94
3.5.2	Equipamentos Activos	95
3.5.3	Equipamentos de Gestão e Segurança	98
3.5.4	Bastidores	98
3.6	Resumo.....	101
4	Conclusões e Trabalho Futuro	102
4.1.1	Trabalho Futuro.....	103
5	Bibliografia	104
6	Anexos.....	106
	Anexo A – Plantas	106
	Anexo B – Medições.....	113
	Anexo C – Orçamento	115

Índice das Figuras

Figura 1. – Organigrama Parcial do ISCED	19
Figura 2. – Tipos de Aplicações	28
Figura 3. – Níveis de Hierarquia e Diversidade na Rede	33
Figura 4. – Hierarquia adicionada à Rede	34
Figura 5. – Algumas Topologias Físicas mais comuns	37
Figura 6. – Modelo Hierárquico da Rede	40
Figura 7. – Exemplo de fluxo agregado	52
Figura 8. - Exemplos de Modelos de Fluxos	54
Figura 9. – Exemplos de equipamentos.....	62
Figura 10. – Vista aérea do ISCED	71
Figura 11. – Modelo Geral da Interligação da Rede	72
Figura 12. – Locais das Aplicações	74
Figura 13. – Fronteiras dos Fluxos e seus respectivos Tipos de Fluxos	83
Figura 14. – Caracterização do Fluxo para a Primeira e Segunda Fronteiras	85
Figura 15. - Arquitectura Lógica da Rede	88
Figura 16. – Subrede do Edifício A.....	89
Figura 17. – Subrede do Edifício B	89
Figura 18. – Subrede do Edifício C	90
Figura 19. – Arquitectura Lógica com Redundância da Rede	91
Figura 20. – Localização dos Bastidores em cada Edifício.....	99
Figura 21. – Exemplos de Bastidores <i>rack</i> de 19”	100
Figura 22. – Planta do 2º Andar do Edifício Principal	107
Figura 23. – Planta do 1º Andar do Edifício Principal	108
Figura 24. – Planta da Cave do Edifício Principal	109
Figura 25. – Planta do 2º Andar do Edifício do Lar	110
Figura 26. – Planta do 1º Andar do Edifício do Lar	111

Figura 27. – Planta do Laboratório de Informática	112
---	-----

Índice das Tabelas

Tabela 1. – Escalões de Atrasos <i>end-to-end</i>	46
Tabela 2. – Valores para taxas de erros	47
Tabela 3. – Característica do Fluxo	48
Tabela 4. – Exemplos de Fluxos do tipo <i>Best-effort</i>	56
Tabela 5. – Exemplos de Fluxos de Áudio e Vídeo Adaptativos	57
Tabela 6. – Classificação dos Sistemas de Medições de Fluxos de Tráfego	60
Tabela 7. – Grupos de Utilizadores	64
Tabela 8. – Grupo de Utilizadores por Necessidade de Aplicação	68
Tabela 9. – Requisitos dos Dispositivos por Aplicação	69
Tabela 10. – Percentagem de Tráfego por Tipo de Aplicação	75
Tabela 11. – Caracterização dos Grupos de Utilizadores	77
Tabela 12. – Localização dos Postos de Trabalho	80
Tabela 13. – Localização dos Postos de Trabalho Actuais e Futuros	81
Tabela 14. – Cálculo dos Fluxos da Rede	84
Tabela 15. – Dimensionamento de Débito em ligações LAN	86
Tabela 16. – Identificação das VLANs	93
Tabela 17. – Quantidades de Equipamentos Passivos	113
Tabela 18. – Quantidades de Equipamentos Activos	114
Tabela 19. – Orçamento do Equipamento Passivo	115
Tabela 20. – Orçamento Equipamento Activo	116

Índice das Fórmulas

(1) – Cálculo do Débito Nominal	56
(2) – Cálculo do Débito de Excepção.....	57
(3) – Cálculo do Atraso máximo <i>round-trip</i>	58

1 Introdução

O ensino é fundamental para o desenvolvimento de uma sociedade. Com ele podemos transmitir conhecimentos de geração em geração e assim educar e aperfeiçoar as capacidades humanas. O processo de ensino-aprendizagem denota, na maioria dos casos, um esforço permanente na busca de soluções que facilitem a vida da sociedade. Algumas dessas soluções dedicam-se a proporcionar uma melhor aprendizagem, enquanto outras aproveitam soluções já existentes de partilha de informação para o ensino, como é o caso da Internet. Das funções pedagógicas fazem parte a selecção e adaptação dos métodos e das técnicas mais adequadas ao ensino. Algumas dessas selecções baseiam-se nas tecnologias de comunicação que permitem efectuar a partilha de informação existente num conjunto de sistemas ligados entre si, de forma a proporcionar uma melhor aprendizagem.

Neste contexto, cada vez mais se tem sentido a necessidade de que num campus universitário haja uma estrutura de rede de comunicações que possibilite uma partilha de informação eficaz dentro e fora da instituição de ensino. Parte dessa estrutura de rede deve permitir o acesso à Internet, bem como a outros serviços que possam ser usados para partilha de conhecimento. A rede de comunicações numa instituição de ensino altera, de forma radical, a concepção tradicional dos instrumentos e ferramentas pedagógicos tradicionais. Ao criar uma estrutura de rede com acesso à Internet numa instituição de ensino, facilita-se a pesquisa de informação, bem como o seu intercâmbio entre professores, estudantes e de professores e estudantes.

O Instituto Superior de Ciências da Educação (ISCED) do Lubango, em Angola, tem necessidade de uma estrutura de rede que suporte e facilite a aprendizagem e

melhore os métodos de ensino. O ISCED é uma instituição vocacionada para formação superior de docentes. Esta instituição de ensino possui já uma rede de comunicações, mas cresceu de forma desorganizada e sem qualquer hierarquia. O único serviço que esta rede disponibiliza aos seus utilizadores é a partilha de Internet, com uma qualidade de serviço fraca e intermitente.

O ISCED, como instituição de ensino, reúne grupos bem definidos de elementos que desempenham um papel activo dentro da instituição, como se pode ver na Figura 1. Estes grupos podem ser agrupados em: docentes, estudantes e funcionários. Estes grupos desempenham várias funções dentro da instituição.

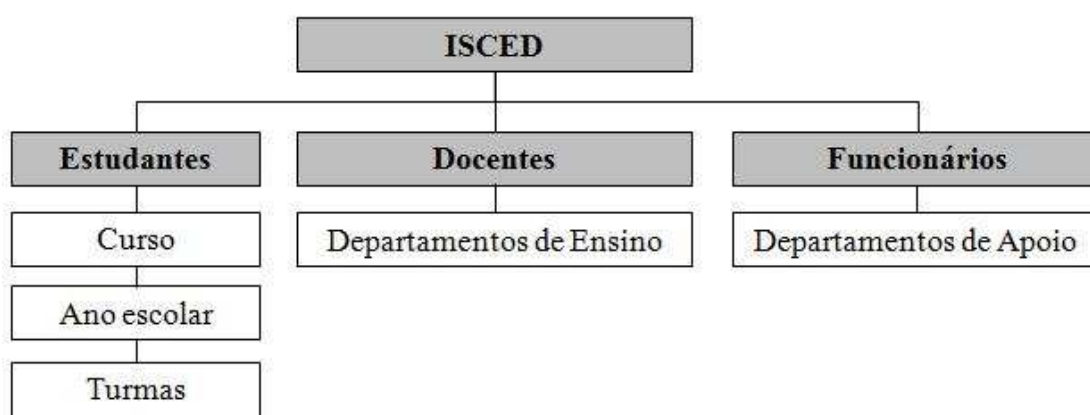


Figura 1. – Organograma Parcial do ISCED

Os docentes encontram-se associados a departamentos de ensino. Nesses departamentos de ensino existem várias repartições que reúnem os docentes que leccionam na mesma área de ensino. Por exemplo, o Departamento de Ciências Exactas é constituído por várias repartições: Informática, Matemática, Química e Física. Assim os docentes encontram-se agrupados segundo uma estrutura construída com base na sua formação disciplinar.

No caso dos funcionários da Instituição, estes podem ser administrativos ou de apoio. Os funcionários administrativos estão ligados à parte burocrática da Instituição, como é o caso da secretaria, dos recursos humanos ou de aprovisionamentos. Os funcionários de Apoio estão ligados à aquisição de stocks (compradores), motoristas e limpeza.

Relativamente aos estudantes, todos desempenham a mesma função dentro da instituição que é a de desenvolver capacidades e competências. Os requisitos destes utilizadores a nível da rede são idênticos entre si. Funcionários administrativos, docentes e estudantes têm necessidades comuns, nomeadamente no que respeita a serviços de email, Web e transferência de ficheiros.

O objectivo deste projecto é criar uma rede de comunicações para o ISCED, de modo a colmatar as falhas da rede actual e a acrescentar serviços que melhorem a qualidade de ensino da instituição, bem como a sua capacidade de partilhar conhecimentos. Dado que a rede existente tem muitas debilidades, será proposta uma nova estrutura da rede assumindo-se que não existe nenhuma rede instalada. Pretende-se que a nova rede tenha uma boa capacidade de expansão e evolução.

Para realizar este projecto, foi necessário fazer primeiro o levantamento dos requisitos, do ponto de vista dos utilizadores, aplicações e dispositivos de rede. Nos requisitos dos utilizadores, consideraram-se os tipos de utilizadores existentes na instituição e as suas necessidades em termos de funcionalidades/serviços de rede. Fez-se depois a análise dos fluxos de tráfego para esta rede, tendo em conta o tipo e orientação dos fluxos nos vários níveis da rede. Assim, com base nessa análise de fluxos fez-se o dimensionamento das ligações, mostrando-se as necessidades de capacidade das ligações. Finalmente, propôs-se a arquitectura lógica da rede. Nesta arquitectura foi necessário garantir redundância na rede, de modo a torná-la mais fiável.

1.1 Objectivos e Metodologia

O objectivo principal desta dissertação é projectar uma rede de comunicações para o ISCED. Num projecto desta natureza existem várias actividades que necessitam de ser executadas, sendo a primeira a recolha de informações sobre o que o cliente pretende, ou seja, os requisitos do cliente, identificando quais os objectivos gerais do projecto.

Seguidamente deve ser efectuado o projecto lógico da rede, no qual se planeiam todos os detalhes a serem implementados e utilizados na rede. Exemplos de aspectos a planear são a topologia da rede, o esquema de endereçamento, os protocolos a utilizar e os softwares de segurança e gestão necessários. Depois do projecto lógico da rede vem o projecto físico da rede. Nesta actividade são escolhidos a tecnologia, os dispositivos e os equipamentos a utilizar, tais como placas de rede, cabos, switches, routers, computadores e impressoras.

A actividade a que se segue é a realização de testes e ensaios para verificar o correcto funcionamento dos componentes instalados e, se necessário, realizar ajustes ao projecto. Seguidamente faz-se o orçamento. Nele se avalia o custo do projecto de modo a atender à melhor relação custo-benefício. Por último, vem a actividade de documentação do projecto da rede e na qual consta todo o processo de planeamento e concepção da rede.

Tendo em conta estas actividades do processo de projecto de uma rede de comunicação, e identificadas as necessidades mais importantes do ISCED, pode-se agora descrever com mais detalhe os objectivos desta dissertação. Foi, por isso, elaborado um conjunto de objectivos a alcançar, descritos a seguir. Estes objectivos, decorrentes do objectivo principal, são os seguintes:

1. Levantamento dos requisitos da rede de comunicações para o ISCED. Para a realizar este objectivo é necessário efectuar o levantamento dos requisitos dos utilizadores, aplicações, dispositivos e da rede.
2. Dimensionamento da rede de comunicações. Para dimensionar a rede é necessário fazer a caracterização dos fluxos de tráfego e calcular os débitos das ligações.
3. Especificação dos equipamentos de rede. Para alcançar objectivo devem-se efectuar as especificações da cablagem, equipamentos activos e equipamentos de gestão e segurança, de modo poder escolher-se a tecnologia a utilizar.

1.2 Resultados do Projecto

O resultado principal desta dissertação é a proposta da rede de comunicações para o ISCED. Este projecto permite satisfazer um conjunto de metas, das quais se destacam as descritas nos parágrafos seguintes.

Uma das metas era efectuar a interligação entre os vários edifícios da instituição, o que se fez usando ligações de fibra óptica. Outra meta era disponibilizar pontos de acesso para todos os PCs dentro dos edifícios. Esta meta foi atingida através da ligação de vários switches segundo uma arquitectura em árvore desde as salas de aulas e gabinetes até ao router CORE. O número de pontos já inclui pontos de acesso de forma a suportar o crescimento previsto do número de pessoas dentro da instituição.

Também era necessário disponibilizar serviços básicos e de acesso à Internet. Uma ligação à Internet foi disponibilizada através de uma ligação do router CORE para o exterior. Foram disponibilizados serviços de FTP e email a partir de servidores próprios ligados à rede interna da instituição.

Uma das grandes preocupações foi garantir largura de banda. Para isso dimensionaram-se as ligações físicas da rede de modo a que os fluxos de dados que por elas circulam não congestionassem a rede. A largura de banda encontrada para a ligação com maior tráfego foi de 1Gbit/s.

A última das metas foi a de se garantir fiabilidade. Esta meta foi atingida através da adição de redundância nos equipamentos mais críticos da rede, nomeadamente no router CORE e nos switch de entrada dos edifícios.

1.3 Estrutura do Relatório

Este relatório é composto por seis capítulos principais. O primeiro capítulo é a Introdução e nele se faz uma introdução ao trabalho realizado e da necessidade da execução do mesmo, enumeram-se os objectivos e descrevem-se os resultados obtidos.

O segundo capítulo é o do Estado da Arte, dedicado à caracterização do estado actual das redes de comunicações e dos dispositivos que as compõem. Também é efectuada uma breve abordagem aos processos de análise, arquitectura e desenho das redes.

Seguidamente vem um dos capítulos mais importantes deste relatório, o capítulo do Projecto da Rede; este capítulo encontra-se dividido em cinco subcapítulos e nos quais se efectua, respectivamente, o levantamento dos requisitos, o levantamento da topologia da instituição, o dimensionamento dos aspectos relevantes para a estrutura da rede, a especificação dos equipamentos necessários à implementação da rede e a definição da arquitectura lógica da rede.

No capítulo das Conclusões e Trabalho Futuro, o quarto capítulo, apresentam-se os benefícios e dificuldades encontrados no decorrer deste projecto e o trabalho futuro previsto para esta instituição desenvolver.

Os dois últimos capítulos deste documento são o da Bibliografia e dos Anexos e neles são apresentados, respectivamente, a documentação consultada ao longo do projecto, e informação extra do relatório. As plantas dos edifícios, as quantidades necessárias de cada um dos componentes especificados (Medições) no capítulo 3 e uma estimativa de orçamento para a implementação da estrutura de rede representam alguma da informação presente nestes anexos.

2 Estado da Arte

2.1 Análise de Requisitos

2.1.1 Utilizador

Os utilizadores introduzem um conjunto de requisitos de *Timeliness*, Interactividade, Fiabilidade, Qualidade de Apresentação, Adaptabilidade, Segurança, Crescimento Futuro e Custo.

Timeliness é um requisito que define em que limite de tempo tolerável o utilizador é capaz de aceder, transferir ou modificar informação. O limite de tempo tolerável depende da percepção do utilizador do que é atraso no sistema. Aqui, atrasos *end-to-end* e de *round-trip* são uma medida útil.

Interactividade é a medida dos tempos de resposta do sistema e rede quando é necessário que eles interajam activamente com o utilizador. O atraso de *round-trip* é uma medida de interactividade.

Fiabilidade, do ponto de vista dos utilizadores, é o grau de confiança que eles têm no sistema.

Qualidade de Apresentação pode ser a percepção que o utilizador tem em relação a visualização de áudio, vídeo e/ou dados.

Adaptabilidade é a capacidade que o sistema tem para se adaptar as novas necessidades dos utilizadores, como exemplo, a mobilidade.

Segurança, da perspectiva do utilizador, é uma exigência para garantir a confidencialidade, integridade e autenticidade da informação e de recursos físicos, bem como controlo de acesso aos utilizadores e recursos do sistema.

Crescimento Futuro prevê o crescimento dos utilizadores e com isso planear para implantar e utilizar novas aplicações e dispositivos na rede.

Custo refere-se a custos de instalação, manutenção e de operação da rede na perspectiva dos utilizadores e da Instituição.

2.1.2 Aplicações e Serviços

As aplicações possibilitam que os utilizadores tirem proveito das tecnologias, protocolos e serviços de comunicação, bem como das capacidades de processamento de informação, existentes num conjunto de máquinas interligadas em rede.

As aplicações são normalmente ponto-a-ponto entre múltiplos dispositivos. Assim os seus requisitos englobam a rede. No início, nas redes, as aplicações/serviços requeriam conectividade básica e transferência de dados através da rede. Actualmente, há outras exigências das aplicações como a de elevado desempenho ou que tenham comportamentos previsíveis ou garantidos a fim de apoiar os requisitos dos utilizadores.

Tendo em conta os requisitos de serviço e de desempenho podemos distinguir as aplicações que necessitam de serviço previsível ou garantido daquelas que podem usar o serviço de *Best-effort*. As aplicações que não requerem um elevado

requisito de fiabilidade, capacidade de manutenção e disponibilidade, são aplicações de *Best-effort*; as que requerem um elevado requisito de fiabilidade, capacidade de manutenção e disponibilidade, são as chamadas aplicações de *Mission-Critical*. Alguns dos requisitos introduzidos pelas aplicações são a Fiabilidade, Capacidade de Manutenção, Disponibilidade, Capacidade e Atraso.

Fiabilidade é uma medida estatística da frequência de falhas da rede e seus componentes e representa as falhas não programadas do serviço.

Capacidade de Manutenção é uma medida estatística do tempo necessário para restaurar o sistema para o estado de completamente operacional, assim que ocorre uma falha.

Disponibilidade é uma medida de relação entre a frequência de falhas críticas e o tempo que demora a restaurar o serviço.

Capacidade é uma medida da aptidão do sistema em transmitir informação (voz, dados, vídeo, ou combinações destes). Vários termos estão associados à capacidade tais como largura de banda e débito.

Atraso é uma medida de diferença de tempo na transmissão de informação através do sistema, ou seja, o atraso é a diferença de tempo em transmitir uma única unidade de informação (bit, byte, célula, janela ou pacote) da origem para o destino.

As aplicações dividem-se em aplicações em tempo real e as aplicações que não são em tempo real (ou tradicionais), como pode ser visto na Figura 2.

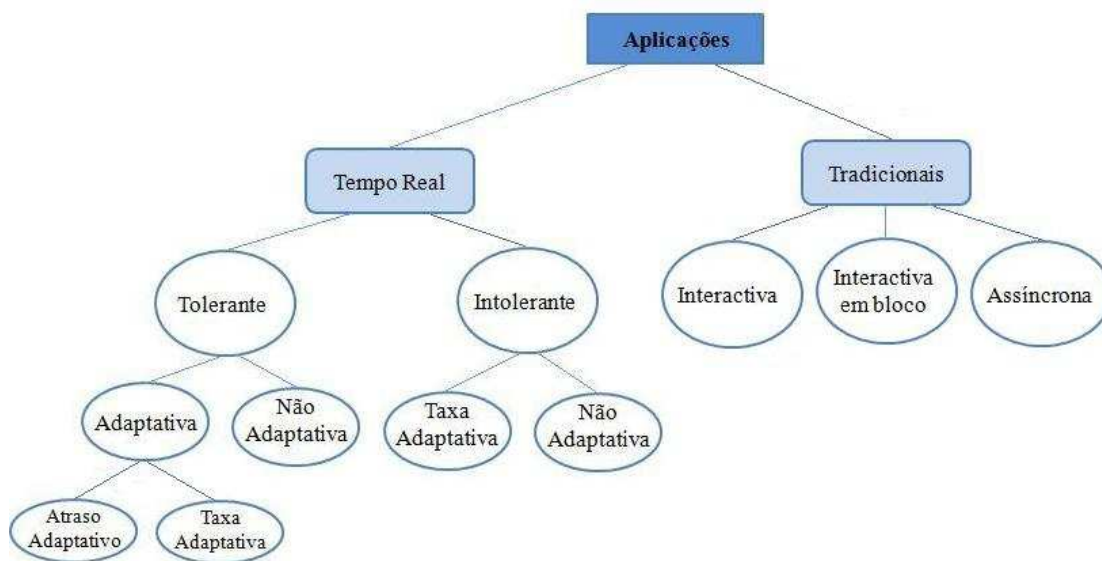


Figura 2. – Tipos de Aplicações

A Internet e a maioria das redes fornecem um modelo de serviço que só é adequado às aplicações tradicionais. Para existirem aplicações em tempo real, como é o caso do áudio e do vídeo, deve-se providenciar um conjunto de especificações a fornecer à rede de modo a que esta garanta qualidade de serviço (*Quality of Service* – QoS) aos utilizadores.

As aplicações possibilitam que um utilizador envie mensagens de correio electrónico, transfira um ficheiro de um servidor para a sua máquina ou participe numa sessão de videoconferência. As aplicações não só fornecem funcionalidades para o utilizador final, mas também constituem a interface entre o utilizador e o sistema de comunicações, tendo a seu cargo funções de identificação e/ou autenticação de utilizadores, a tradução de nomes simbólicos (ex: nomes de máquinas) em valores numéricos com significado para os protocolos utilizados para comunicação. Assim as aplicações são agrupadas em

três categorias: Aplicações *Best-effort*; Aplicações *Continuous-media*; Aplicações Adaptativas.

Aplicações *Best-effort* são aplicações tradicionais de dados tolerantes a variações de débito, atraso e perdas. Aplicações *Continuous-media* são aplicações de acesso remoto a ficheiros, Base de dados, recursos a sistemas informáticos. São aplicações resultantes da integração de serviços em sistemas informáticos. Necessitam de garantias de débito, atraso e perdas. As aplicações Adaptativas são aplicações multimédia que utilizam diferentes tipos de informação como por exemplo, dados, áudio e vídeo.

Também as aplicações podem ser classificadas tendo em conta os requisitos de serviço e desempenho. Nesta perspectiva, as aplicações são classificadas em três categorias: *Mission-Critical*; *Rate-Critical*; e Tempo Real e Interactivas.

Aplicações *Mission-Critical* tem requisitos de Fiabilidade, Capacidade de Manutenção e Disponibilidade previsíveis, garantidos e/ou de alto desempenho. Um veículo comandado remotamente é um exemplo. Aplicações *Rate-Critical* tem requisitos de capacidade previsíveis, garantidos e/ou de alto desempenho. Aplicações de Tempo Real e Interactivas tem requisitos de atraso previsto, garantidos e/ou de alto desempenho. A videoconferência é um exemplo.

2.1.3 Dispositivos

Os dispositivos podem ser agrupados segundo três categorias: dispositivos informáticos genéricos, servidores e dispositivos especializados. Dispositivos Informáticos Genéricos são os *desktop* e *laptop* que a maioria dos utilizadores

utiliza. Este grupo inclui também os dispositivos *handheld*. Servidores são dispositivos informáticos que prestam serviço a um ou mais utilizadores (Clientes). Estes normalmente são mais potentes, em termos de memória, processamento, rede e discos, do que os dispositivos *desktop* ou *laptop* dos utilizadores. Dispositivos Especializados são dispositivos que proporcionam funções específicas para os seus utilizadores (ex: impressora, scanner).

2.1.4 Rede

Uma rede de comunicações é um conjunto de sistemas ligados entre si. Para se efectuar o planeamento de uma rede de comunicações há que, numa primeira fase, efectuar uma análise de requisitos. Numa segunda fase propor uma arquitectura baseada nessa análise de requisitos e numa terceira e última fase projectar ou fazer o desenho da rede. Sendo assim, a análise, arquitectura e desenho da rede são processos usados para produzir desenhos lógicos, reproduzíveis e justificáveis. Estes processos estão interligados devido às trocas de informação existentes entre a análise e a arquitectura e entre a arquitectura e o desenho.

A análise de redes implica apreender o que os utilizadores, suas aplicações e dispositivos necessitam da rede, bem como perceber o comportamento desta sobre várias situações, de modo a definir e determinar as relações entre a rede, utilizadores, aplicações e dispositivos. Ao efectuar a análise da rede, desenvolve-se um conjunto de objectivos que descrevem os problemas que a rede que está a ser projectada irá abordar. Este conjunto de objectivos será baseado nos requisitos e fluxos de tráfego, assim como na localização dos utilizadores, aplicações e dispositivos. Assim, pode-se dizer que a análise de redes ajuda a

compreender que problemas estão a tentar ser resolvidos, compilando informação que será usada no desenvolvimento da arquitectura e do desenho da rede.

A arquitectura da rede usa a informação do processo de análise para desenvolver uma estrutura conceptual, de alto nível da rede. Ao se desenvolver a arquitectura da rede fazem-se escolhas de tecnologia e topologia para a rede e são determinadas as relações entre as funções da rede. Usualmente não existe uma única arquitectura (ou desenho) “correcta” para a rede mas sim várias, das quais umas vão funcionar melhor do que outras em determinados aspectos. O processo de arquitectura e desenho destina-se a encontrar os melhores parâmetros para a arquitectura e desenho da rede de acordo as condições da rede em causa. O desenho da rede fornece o detalhe físico para a arquitectura. Esse detalhe físico inclui plantas e desenhos da rede, selecção de fabricantes e fornecedores de serviços, e selecção de equipamentos.

Estes processos de análise, arquitectura e desenho formam a base para os projectos de redes que podem ser de curto prazo e de longo prazo. Os objectivos de curto prazo são objectivos a ser cumpridos num prazo de, por exemplo, um ano e os de longo prazo são de, por exemplo, cinco anos. Os objectivos de curto e longo prazo poderão ser considerados extensões propostas do projecto actual. O desenho de rede que se está a desenvolver deverá facilmente permitir fazer alterações futuras à rede. O objectivo de longo prazo é uma estimativa rude pois não é possível saber que tecnologias, serviços ou níveis de desempenho estarão disponíveis no futuro, logo, por estes motivos, os objectivos de longo prazo são variáveis.

A análise da rede é importante no sentido em que ajuda a perceber a complexidade e as nuances de cada rede e dos sistemas que elas suportam. A análise também fornece dados que ajudam a garantir a justificação da

arquitectura e desenho resultantes. Duas das características básicas das redes são: os seus níveis de hierarquia e a sua diversidade. A hierarquia é o grau de concentração de fluxos de tráfego em pontos de interligação dentro da rede. As hierarquias providenciam separação e estrutura dentro da rede à medida que esta vai crescendo, e ajudam na determinação dos tamanhos das redes, incluindo encaminhamento e configurações de endereçamento, desempenho, níveis de serviço e tecnologias.

No desenho da rede além de termos em conta a hierarquia devemos também ter em consideração o grau de diversidade (também conhecido como redundância ou interconectividade). A diversidade é importante na medida em que fornece um mecanismo para se atingir maiores desempenhos dentro da hierarquia da estrutura da rede.

A grande importância da hierarquia é o facto dela separar a rede em segmentos, podendo estes segmentos ser redes mais pequenas (sub-redes) ou de *broadcast*. A hierarquia é necessária quando a quantidade de tráfego na rede cresce além da capacidade da rede ou quando as interacções entre os dispositivos da rede resultam em congestionamento. Essa capacidade de crescimento devida à hierarquização da rede é importante nos projectos de curto e longo prazo, visto que fornece um modo de facilmente se poder estender a rede.

A diversidade é importante na medida em que fornece um mecanismo para se atingir maiores desempenhos dentro da hierarquia da estrutura da rede. No processo da análise, arquitectura e desenho da rede deve haver um balanceamento na escolha entre hierarquia e diversidade, que é uma das escolhas fundamentais desse processo.

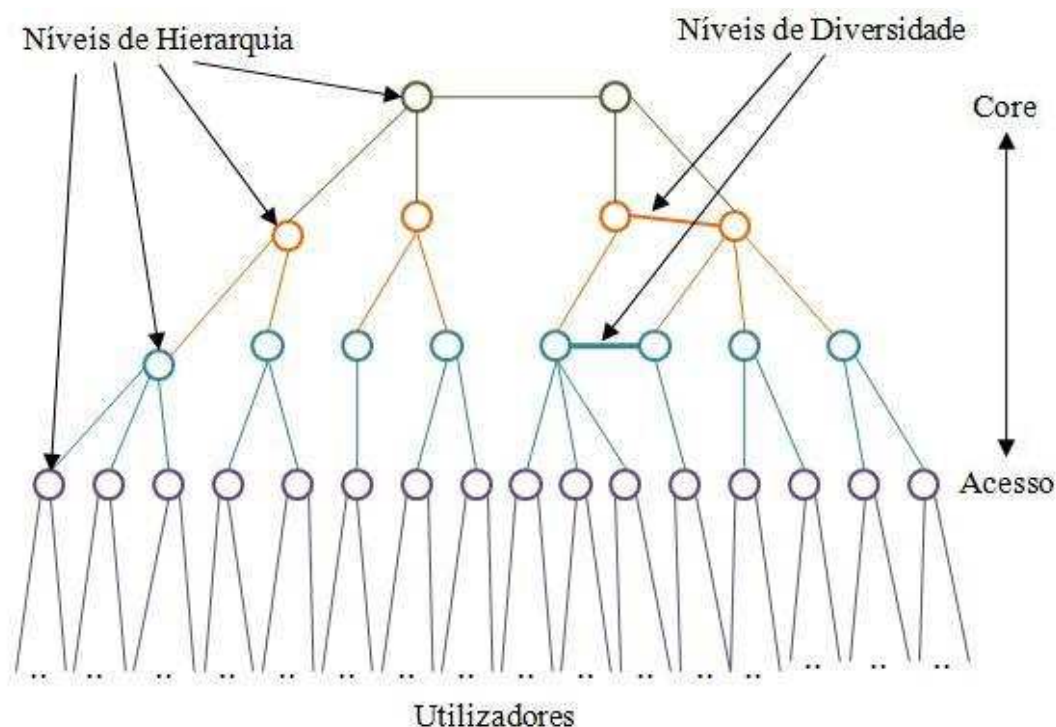


Figura 3. – Níveis de Hierarquia e Diversidade na Rede

A Figura 3 ilustra a árvore típica para uma rede, com os círculos a representar redes ou routers e linhas a representar ligações de comunicações entre redes e/ou routers. Como se pode ver, há 4 níveis de hierarquia, desde as redes de core até às redes de acesso mais próximas dos utilizadores. Alguns métodos de adicionar hierarquia à rede são através da inserção de Encaminhamento, Sistemas Autónomos e Protocolos de *Gateways*.

O método de Encaminhamento adiciona encaminhamento à rede, passando de uma estrutura plana, baseada apenas em switches ou *hubs*, para uma estrutura de encaminhamento, baseada em routers. O método de Sistema Autónomo aplica-se quando se evolui de um sistema autónomo único (AS) para ligações de múltiplos sistemas únicos. E finalmente, o método de Protocolos de *Gateways* é quando se

migra de *Interior Gateway Protocols* (IGP) para *Exterior Gateway Protocols* (EGP) e para políticas baseadas no encaminhamento.

O método de encaminhamento reduz o tamanho do *broadcast* ou o número de dispositivos alcançados por mensagens de *broadcast*. A utilização de routers concentra os fluxos de tráfego e reparte o domínio de *broadcast* em pequenos domínios de *broadcast*, como pode ser observado na Figura 4.

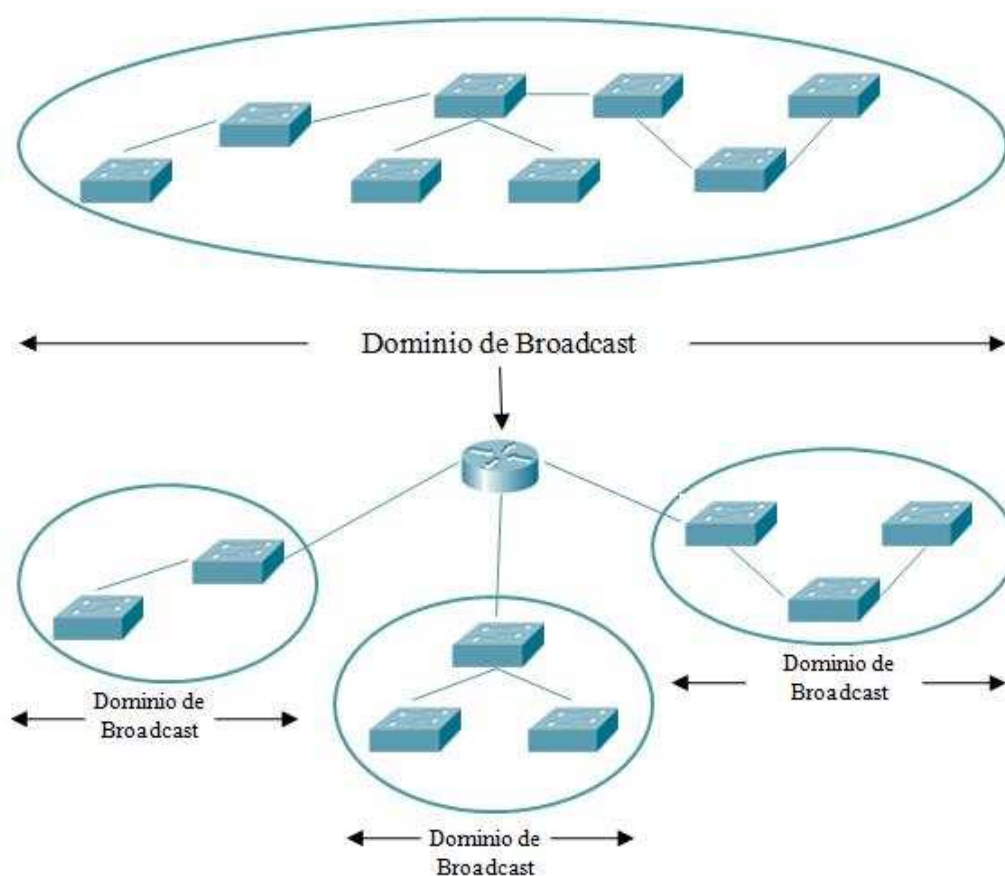


Figura 4. – Hierarquia adicionada à Rede

Um exemplo da adição de diversidade à rede é a Rede de Entrega de Conteúdos (CDN). Uma CDN evita o core da rede onde há maior probabilidade de ocorrer congestionamento e liga directamente dispositivos ou redes que se encontram num patamar inferior de hierarquia. Isso proporciona um melhor desempenho mas pode afectar a hierarquia da rede ao modificar o seu comportamento de encaminhamento.

Regra geral, os requisitos para a arquitectura da rede têm em conta os requisitos, serviços e características de redes já existentes que serão incorporadas com esta nova rede. Alguns requisitos essenciais da rede são a Disponibilidade, Fiabilidade, Gestão, Segurança e Atraso.

Disponibilidade é a fracção de tempo em que o sistema (hardware e software) está operacional. Uma medida comum de disponibilidade é expressa em termos de percentagem de *uptime* e *downtime*

Fiabilidade é um indicador da ocorrência de falhas de uma ligação. Quanto mais fiável, menor número de falhas se espera que possam ocorrer na ligação.

Gestão consiste na monitorização da operabilidade dos recursos da rede com o objectivo de determinar potenciais falhas e problemas, bem como ajustar a arquitectura e as configurações dos dispositivos, de forma a otimizar a utilização da rede

Segurança procura minimizar os problemas associados ao acesso não autorizado a recursos da rede.

Atraso refere-se ao tempo gasto para transmitir um pacote através de um determinado meio. O atraso depende do meio de transmissão, da distância entre a origem e o destino e da congestão da rede.

2.1.4.1 Arquitectura

Uma arquitectura de rede é um modelo abstracto que permite descrever a organização e o comportamento dos sistemas que constituem a rede. Este modelo abstracto baseia-se num conjunto de princípios gerais e define regras de funcionamento, permitindo descrever de forma clara e concisa conceitos e relações essenciais entre os componentes da rede. Os diferentes dispositivos que constituem a estrutura de rede podem ser interligados sob várias formas, tanto do ponto de vista físico (topologia física) como do ponto de vista lógico (topologia lógica). De um modo básico, podemos definir a topologia como sendo um mapa da rede.

Segundo [4], a topologia física da rede descreve o posicionamento físico dos cabos, postos de trabalho e a localização de todos os equipamentos da rede. Por vezes as topologias físicas são comparadas com as topologias lógicas, que definem a forma como a informação circula na rede. Normalmente as duas topologias são similares. No entanto, podem ser diferentes. Na Figura 5 são apresentadas algumas topologias físicas mais comuns.

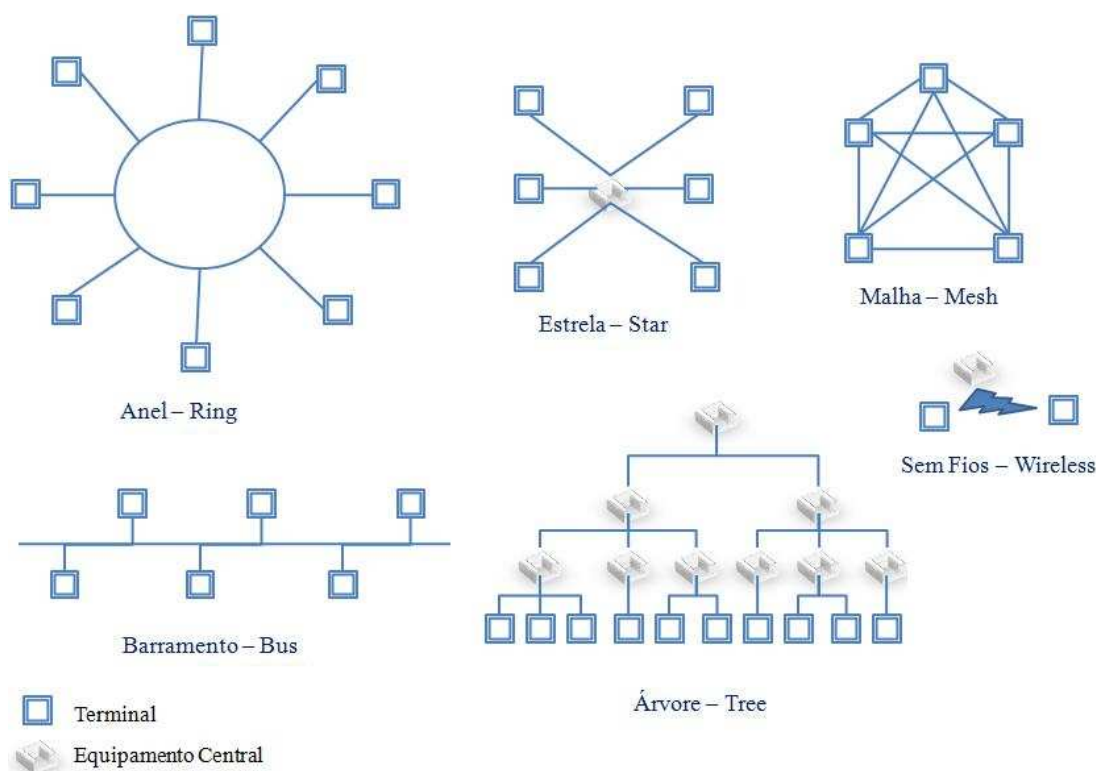


Figura 5. – Algumas Topologias Físicas mais comuns

A determinação de como os diferentes dispositivos vão ser ligados numa rede pode ser um ponto crítico, pois uma má escolha da topologia física e um mau aproveitamento dos recursos da rede, poderão resultar numa reestruturação e aquisição de novos equipamentos, o que se irá reflectir em termos de orçamento e desperdício de verbas. A topologia da rede depende do projecto, da fiabilidade esperada e do seu custo operacional. Para simplificar o processo de comutação e explorar topologias mais simples, as redes LAN utilizam topologias em barramento (*bus*), estrela (*star*), anel (*ring*) e/ou árvore (*tree*).

De modo a garantir elevados níveis de fiabilidade, disponibilidade, flexibilidade e robustez da estrutura da rede, as redes WAN adoptam topologias em malha (*mesh*), que permitem explorar rotas alternativas entre dispositivos, de forma a

garantir continuidade de serviço mesmo em caso de falhas dos dispositivos e ligações entre dispositivos e permitir distribuição de tráfego, explorando a capacidade de ligações menos sobrecarregadas.

No desenvolvimento de redes LAN pode-se querer melhorar a fiabilidade da rede com ligações redundantes entre switches e routers. Segundo [6], a interligação de dispositivos através de uma rede com ligações redundantes apresenta vantagens relativamente a uma rede sem redundância porque se um dos caminhos for cortado a trama pode seguir por outro caminho. Contudo, o comportamento de uma rede com redundância apresenta alguns problemas, que se não forem resolvidos degradam o desempenho da rede ao ponto da sua utilização se tornar inviável. *Broadcast*, Caminho e Tabela de endereçamento são alguns problemas com a utilização da redundância na rede.

Os problemas provenientes do *broadcast* são devidos aos switches não filtrarem os pacotes de *broadcast*, ou seja, todos os *broadcasts* recebidos por uma interface são enviados para todas as restantes interfaces. Isto quer dizer que se tivermos muitas ligações entre switches, ao receberem o pacote de *broadcast* todos os switches teriam o mesmo comportamento e assim o pacote seria transmitido indefinidamente na rede

Adicionando redundância na rede passará a existir mais de um caminho entre dois dispositivos, o que quer dizer, que um qualquer dispositivo poderá receber várias cópias da mesma *trama*. Ter várias cópias de uma *trama* a percorrer a rede significa a utilização ineficiente da largura de banda

Quanto à Tabela de Endereçamento, pode acontecer que tenha de estar constantemente a alterar a tabela à medida que vai recebendo *tramas* de uma

máquina por interfaces diferentes. Sendo assim, o switch poderá passar o tempo a alterar a tabela de encaminhamento.

Para evitar estes problemas e ao mesmo tempo garantir redundância de ligações, foi criado o protocolo *Spanning Tree Protocol* (STP), que veio dar origem à norma IEEE 802.1D. A ideia básica do STP é eliminar ciclos lógicos da rede. O protocolo STP começa por eliminar os ciclos lógicos de rede e depois mantém uma monitorização constante da rede. Sempre que uma ligação adicional crie um ciclo, o STP reinicia o processo de eliminação de ligações lógicas redundantes. O STP garante que numa rede com redundância haverá apenas um caminho entre duas quaisquer máquinas. Se por qualquer razão não for possível a transmissão entre duas máquinas pelo caminho actual, o STP inicia um processo de activação de um caminho redundante, no caso de existir redundância física. Durante o processo de activação do novo caminho, o STP tem de garantir que não ocorram ciclos.

Uma das vantagens deste protocolo é o facto de garantir que uma rede assume sempre uma topologia lógica em árvore, o que resulta na existência de um caminho único entre dois dispositivos, numa rede baseada em switches. Outra vantagem é que este protocolo garante uma elevada tolerância a falhas, permitindo que a rede se reconfigure automaticamente na situação de falha de uma ligação

2.1.4.2 Hierarquia

A definição da hierarquia da rede propõe um modelo hierárquico para o projecto de modo a implementar uma estrutura de comunicação fiável e eficiente. Pode ser observado na Figura 6, que o modelo hierárquico está dividido em três camadas lógicas: camada central ou CORE, a camada de distribuição e a camada de acesso.

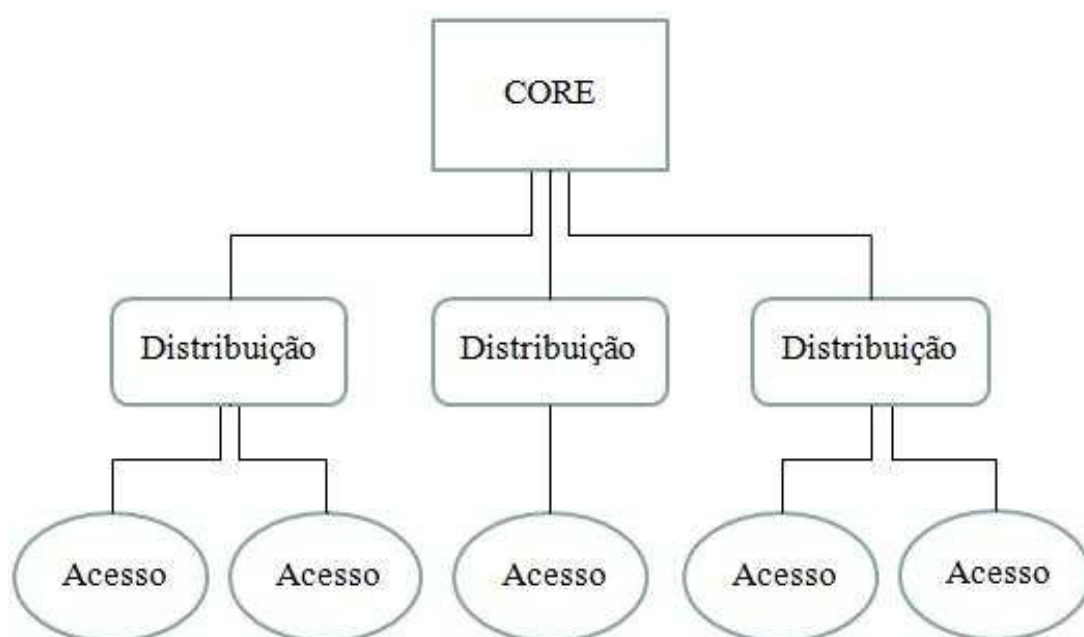


Figura 6. – Modelo Hierárquico da Rede

A camada central é a estrutura principal da rede, e a sua principal função é transportar grandes quantidades de dados o mais depressa possível sem quaisquer restrições sobre fluxos de dados. Como todos os utilizadores usam os serviços desta camada então é importante incluir tolerância a falhas, recorrendo, entre outras opções à redundância de dispositivos e ligações.

A comunicação entre a camada central e a camada de distribuição deve ser feita com meios físicos de transmissão com grande largura de banda, geralmente, implementados com fibra óptica. A camada de distribuição estabelece o elo de ligação entre a camada central e a camada de acesso. Tem as funções de encaminhamento dos dados entre a camada central e camada de acesso, implementação de políticas de segurança, controlo de acesso, definição dos domínios de *broadcast*, etc. A camada de acesso é formada pelos dispositivos de ligação dos postos de trabalho à rede, switches e *hubs*. Esta camada também inclui funções de controlo de acesso e definições de domínio de colisão. A camada de acesso é formada principalmente por switches.

2.1.4.3 Endereçamento

Os dispositivos ligados a rede são identificados com um endereço lógico. O endereço lógico é composto por dois componentes; um componente de identificação da rede e outro de identificação do dispositivo. Deste modo, consegue-se agrupar logicamente todos os dispositivos que pertencem a uma rede. Assim, quando se pretende encaminhar um pacote para um dispositivo remoto, o router apenas tem de conseguir encaminhar o pacote até à rede remota a que pertence o dispositivo.

Para simplificar o processo de endereçamento, os números que compõem os endereços são subdivididos em campos. Com base na subdivisão do endereço lógico, podem ser criados vários esquemas de endereçamento com tamanhos e identificadores diferentes para cada um dos campos do endereço. Em todos eles, deve procurar-se um esquema de endereçamento que suporte redes de grande dimensão, com um grande número de dispositivos por rede, e que suporte um

grande número de redes. O esquema de endereçamento também deve considerar a possibilidade de com um único endereço fazer referência a todos os dispositivos de uma rede (endereço de *broadcast*) ou a um grupo específico de dispositivos (endereço de *multicast*).

Todos os dispositivos que pretendem comunicar através de uma rede TCP/IP devem ser identificados por um endereço lógico ou endereço IP. A versão 4 do protocolo IP considera endereços lógicos com 32bits divididos em quatro grupos de 8bits cada. O Endereço IP é indicado com o valor dos 4 grupos separados por um ponto, ou seja, o endereço é representado em formato binário mas para facilitar a interpretação esse valor é convertido em formato decimal pontuado, por exemplo:

$$11000000.10101000.00001001.00000000_{(2)} = 192.168.9.0_{(10)}$$

A Internet é um conjunto de diversas redes independentes que trocam tráfego usando o protocolo IP. Cada uma destas redes possui um conjunto de endereços IP representados pelo endereço e máscara de rede. Este par é composto por um prefixo/tamanho, onde o prefixo representa o endereço de rede e o tamanho indica o número de bits que corresponde à máscara de rede associada a esta rede. Por exemplo 192.168.1.0/24

2.1.4.4 VLAN

Segundo [2], com VLAN é possível definir diferentes grupos de utilizadores e/ou servidores que comuniquem exclusivamente entre si, constituindo redes virtuais distintas das existentes dentro da mesma rede física. As VLANs são redes locais

logicamente independentes entre si, com isolamento de tráfego *unicast* e *broadcast*.

Uma VLAN é um domínio de *broadcast* criado com um ou mais switches. Quando se criam VLAN num switch, estão-se a criar várias redes, uma por VLAN, cada uma com o seu domínio de *broadcast*, isto segundo [6]. Os dispositivos pertencentes a uma dada VLAN não necessitam de estar ligados ao mesmo switch, pode-se criar vários domínios de *broadcast*.

As VLANs possuem algumas vantagens de utilização. Os *broadcasts* de VLANs diferentes são filtrados, por defeito, pelo switch e, com isso, reduzem-se os efeitos negativos dos *broadcasts*. Quando se cria uma VLAN especificam-se as portas do switch pertencem à VLAN e a que recursos essas portas podem aceder tornando as redes mais seguras. Com a utilização de VLAN garante-se flexibilidade na rede, ou seja, pode-se adicionar um utilizador a uma qualquer VLAN independentemente da sua localização física. Com a utilização de VLAN não é preciso necessariamente um switch por domínio de *broadcast*. Um switch é suficiente para suportar vários domínios de *broadcast* e, consequentemente, várias redes com endereços diferentes, o que poderá permitir uma redução dos custos.

2.1.5 QoS

Hoje em dia, as aplicações necessitam que uma rede tenha a capacidade de dar suporte adequado a uma variedade de tráfego com determinados requisitos de desempenho. De modo a garantir qualidade para estas aplicações, a rede deverá ter requisitos especiais de qualidade de serviço (QoS). As necessidades das

aplicações são expressas através de um conjunto de parâmetros de QoS. Fazem parte desse conjunto de parâmetros de QoS, o débito binário, o atraso e as perdas ou taxa de erros.

2.1.5.1 Débito

O débito é uma medida da quantidade de bits que atravessam um canal de comunicação por unidade de tempo. Este é o primeiro parâmetro de QoS a condicionar o desempenho da rede. Os serviços para as aplicações de tempo real e algumas aplicações tradicionais têm requisitos de débito específicos que, se não forem satisfeitos, impedem o normal funcionamento da aplicação. As classes das aplicações em termos de débito binário podem ser caracterizadas por *Constant Bit Rate* (CBR), *Variable Bit Rate* (VBR), *Available Bit Rate* (ABR) ou *Unspecified Bit Rate* (URB).

As aplicações CBR têm necessidades de débito constante, como por exemplo áudio ou vídeo não comprimido. Também são designadas por serviços *Continuos Media*. As aplicações VBR têm necessidades de débito caracterizadas por um valor médio e por um valor de pico como, por exemplo, vídeo comprimido. Também são designadas *Continuos Media*, uma vez que é apenas uma variante comprimida deste tipo de serviço.

As aplicações ABR têm necessidades indefinidas de débito, como por exemplo vídeo *on demand* e dados. Também são designadas por serviços Adaptativas. E, finalmente, UBR destina-se às aplicações sem quaisquer requisito e/ou garantias de largura de banda para as quais basta que a rede garanta o transporte de informação. São também designadas por serviços *Best-effort*.

O débito médio é a taxa média de transmissão/recepção de bits medida ao longo do intervalo de tempo correspondente à duração do fluxo de informação. O débito de pico é o débito máximo registado durante um curto intervalo de tempo

2.1.5.2 Atraso

No sentido mais básico, o Atraso é a diferença de tempo entre transmitir uma única unidade de informação (bit, byte, célula, janela ou pacote) da origem para o destino. Existem várias fontes de atrasos tais como propagação, transmissão, filas de espera e processamento. O atraso pode ser medido num sentido (*end-to-end*) e em ambos os sentidos (*round-trip*). Ambas as medidas de atraso são úteis, contudo apenas os atrasos de *round-trip* podem ser medidos com o uso da ferramenta prática e universalmente disponível chamada *ping*.

Outra medida de atraso incorpora o processamento de dispositivos e aplicações, tendo em conta o tempo que leva a executar a tarefa. À medida que o tamanho da tarefa aumenta, os tempos de processamento da aplicação (e portanto os tempos de resposta do sistema) também aumentam. Este tempo de atraso, também chamado latência, pode ser importante para o comportamento da aplicação e da rede. A latência também pode ser usada para descrever o tempo de resposta de um dispositivo de rede.

A variação do atraso (*jitter*) é a mudança do atraso ao longo do tempo e é uma característica importante para aplicações e fluxos de tráfego que requerem atraso constante. Por exemplo, aplicações de tempo real e quase tempo real muitas vezes requerem uma variação do atraso rigorosa. Juntos, atraso e variação do atraso, ajudam a descrever o comportamento da rede.

A *International Telecommunications Union* ITU-T na sua recomendação G.114 define, como se pode ver na Tabela 1, os seguintes escalões de atraso máximo *end-to-end*.

Tabela 1. – Escalões de Atrasos *end-to-end*

Escalões	Descrição
< 150 ms	Atrasos aceitáveis para a maioria das aplicações
≥ 150 e < 400 ms	Atrasos com impacto em algumas aplicações
> 400 ms	Atrasos inaceitáveis no planeamento de redes de telecomunicações

2.1.5.3 Perdas ou Taxa de Erros

Numa rede de dados há dois factores essenciais que originam os erros ou perdas. O primeiro factor é o erro na transmissão/recepção de bits, o que provoca a eliminação dos pacotes de dados que contêm esses erros. O segundo factor é a eliminação de pacotes de dados devido o congestionamento da rede ou de alguns dos seus elementos. O primeiro factor vem sendo ultrapassado com a evolução das tecnologias de redes. O segundo factor é responsável pela grande parte das perdas, uma vez que a eliminação dos pacotes de dados é frequentemente devido a falta de recursos, como por exemplo, a falta de espaço em filas nos switches. A Tabela 2 mostra alguns valores para as taxas de erros

Tabela 2. – Valores para taxas de erros

Valor	Descrição
10^{-4}	Utilizado para aplicações de voz e aplicações não interactivas de transferência de dados
10^{-6}	Utilizado para aplicações interactivas de transferência de dados
10^{-7}	Utilizado para aplicações de transferência de imagens
10^{-8}	Utilizado para aplicações de transferência interactiva de imagens comprimidas

2.2 Análise de Fluxos

Para se projectar uma rede de comunicações eficiente e aplicar as melhores práticas de gestão, devem-se efectuar análises e medições de fluxos. Um fluxo pode ser caracterizado como um conjunto unidireccional de pacotes IP com o mesmo endereço de origem e destino, mesmo número de porta e mesmo protocolo. Segundo [1], o fluxo é um conjunto de pacotes de tráfego gerado por aplicações. Estes pacotes têm atributos comuns tais como endereços de origem/destino, tipo de informação, direccionalidade ou outra informação *end-to-end*.

Uma vez que os fluxos são *end-to-end*, eles podem ser directamente ligados às aplicações, dispositivos ou equipamentos da rede. Eles também podem ser associados ao utilizador final. A medição na fase de planeamento da rede é efectuada em termos de estimativa dos fluxos das aplicações, enquanto que a medição real dos fluxos de tráfego deverá ser feita depois da rede montada e com auxílio de software de monitorização.

A análise dos fluxos é o processo de caracterizar os fluxos de tráfego de uma rede, onde estes são susceptíveis de ocorrer, e que níveis de desempenho irão exigir. Ao efectuar a análise de fluxos não é possível mostrar todos os fluxos em uma rede, mas sim os fluxos que terão maior impacto sobre a arquitectura e desenho da rede. Isto resulta que apenas uma pequena parte do total do conjunto dos fluxos de uma rede é realmente analisado.

Análise dos fluxos é útil para compreender o comportamento das redes existentes, planear o desenvolvimento e expansão da rede, quantificar o desempenho da rede, verificar a qualidade de serviço e conhecer a utilização da rede ou subrede por parte de cada utilizador. São indicadas algumas características dos fluxos na Tabela 3.

Tabela 3. – Característica do Fluxo

Característica do Fluxo	
Requisitos do Desempenho	Capacidade
	Fiabilidade
	Disponibilidade
	Atraso
	QoS
Níveis Importância / Prioridade	Negócio / Empresa / Fornecedor
	Politica
Outros	Direccionalidade
	Conjuntos comuns de utilizadores, aplicações, dispositivos
	Calendarização (<i>Scheduling</i>)
	Protocolos usados
	Endereços / portas
	Requisitos de Segurança /Privacidade

A análise de fluxo fornece conhecimento sobre os graus de hierarquia e diversidade necessários na arquitectura e desenho da rede [1]. Esta análise também fornece informação que pode ser útil na escolha dos routers, switches ou mecanismos híbridos. A agregação dos requisitos e fluxos na rede, devidos à hierarquia, levam a fluxos agregados e isto pode acontecer tanto na rede de acesso como na rede de *backbone* (core).

Os fluxos podem ser do tipo Individual, Agregado ou de *Backbone*. Fluxo do tipo Individual é o fluxo associado a uma única aplicação. Fluxo do tipo Agregado é a combinação de vários fluxos individuais que partilham a mesma ligação, caminho ou rede. Fluxo do tipo *Backbone* é a combinação de vários fluxos agregados, quando a rede atinge um certo grau de hierarquia.

Quando se efectua um projecto de rede tendo em conta o planeamento de capacidade dessa rede, a maioria dos fluxos identificados é do tipo *best-effort*. Segundo [10], um método de identificar fluxos numa rede é determinar onde estão as fontes e destinos dos dados. As fontes são os dispositivos ou grupos de dispositivos que produzem dados e o destino são os dispositivos ou grupos que recebem dados da rede. A identificação das fontes e destinos dos fluxos irá indicar as fronteiras dos fluxos que poderá ser entre andares num edifício, entre edifícios num *campus*, entre *campus*, entre uma LAN e uma WAN.

2.2.1 Tipos de Fluxos

2.2.1.1 Fluxos Individuais

O fluxo individual é um fluxo para uma única sessão de uma aplicação. Os fluxos de requisitos garantidos podem ser tratados separadamente do resto dos fluxos. A caracterização dos fluxos das aplicações deve ser realizada isoladamente, nos postos de trabalho dos utilizadores e considerando os agregados de fluxos, nos acessos aos servidores e nas ligações dos níveis hierárquicos superiores.

Essa caracterização de fluxos deve ser feita em termos de necessidade de débito (médio e de pico), atraso (máximo e variação) e perdas. Enquanto que para as aplicações *Continuos media* a definição destes parâmetros não apresenta grandes dificuldades, uma vez que se tratam de aplicações com características e necessidades de fluxos geralmente bem conhecidas, o mesmo não acontece com as aplicações *Best-effort* e as Adaptativas, pois nestes tipos de aplicações não existem valores determinados para os parâmetros de caracterização dos fluxos mas sim intervalos de funcionamento relativamente latos, dentro dos quais as aplicações têm um comportamento dentro do esperado.

Os intervalos de funcionamento dos parâmetros das aplicações *Best-effort* podem ser definidos através da quantificação das expectativas dos utilizadores em relação ao comportamento das aplicações e estas respostas podem ser obtidas através da realização de inquéritos aos utilizadores. Por motivos de eficiência, esta caracterização é efectuada pela equipa de projecto com base nos requisitos identificados e na experiência de situações anteriores.

O tamanho dos blocos de dados trocados em cada transacção entre o emissor e receptor na rede, é um elemento importante na caracterização dos fluxos *Best-effort*. A obtenção deste elemento pode ser feita de forma precisa para cada par utilizador/aplicação ou de forma genérica para o conjunto das aplicações usadas na infra-estrutura.

Ao contrário da caracterização de fluxos de aplicações *Best-effort*, as aplicações Adaptativas requerem um conhecimento preciso dos parâmetros óptimos de funcionamento em função do nível de qualidade pretendida. As aplicações Adaptativas resultam da necessidade de transportar os fluxos de aplicações do tipo *Continuos media* em sistemas de comunicação sem capacidade de garantia estrita de níveis de QoS.

2.2.1.2 Fluxos Agregados

Segundo [1], um fluxo agregado é uma combinação de múltiplas aplicações ou de fluxos individuais, que partilham uma ligação, caminho, ou rede comuns. Grande parte dos fluxos numa rede são fluxos agregados. A Figura 7 exemplifica alguns fluxos agregados.

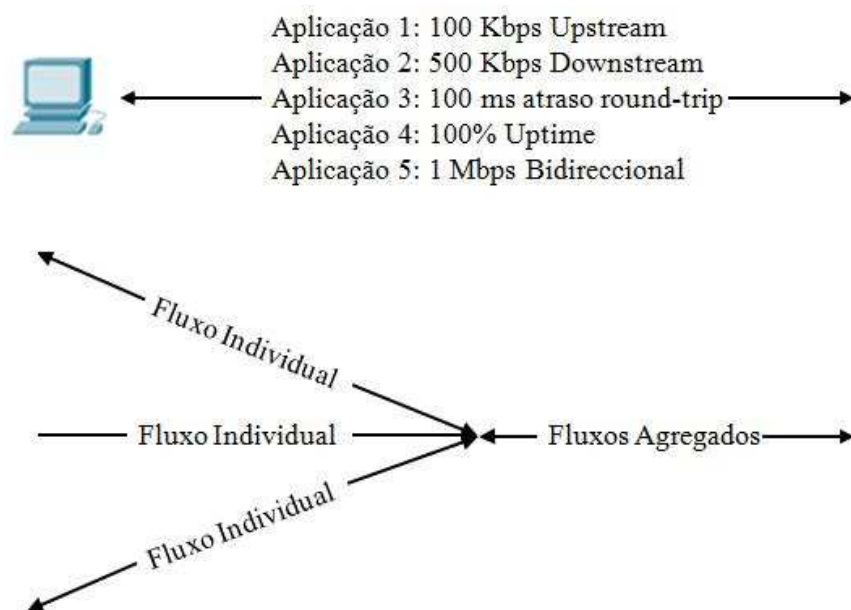


Figura 7. – Exemplo de fluxo agregado

Os fluxos bidireccionais podem ser considerados fluxos individuais, um de *upstream* e outro de *downstream*. O *upstream* indica o sentido do fluxo em direcção à origem, normalmente o Core da rede, e o *downstream* indica o sentido do fluxo em direcção ao destino, que pode ser a periferia da rede (dispositivos do utilizador).

2.2.2 Modelos de Fluxos

Um método utilizado para descrever os fluxos na rede é compará-los com modelos de fluxos bem conhecidos. As principais características dos modelos de fluxo são a direccionalidade, a hierarquia e a diversidade. A direccionalidade descreve a preferência de um fluxo em ter mais requisitos numa direcção do que

noutra. Tipicamente as arquitecturas e desenhos de redes, tratam o fluxo de tráfego como tendo requisitos iguais em ambas as direcções mas, especialmente para aplicações mais recentes, existem requisitos substancialmente diferentes em cada direcção (fluxos assimétricos). Os modelos de fluxo ajudam a descrever os graus de hierarquia e diversidade dos fluxos para aplicações. Há quatro modelos de fluxos mais utilizados: *Peer-to-Peer*, Cliente-Servidor, Cliente-Servidor hierárquico e Computação Distribuída.

No modelo *Peer-to-Peer* todos os dispositivos se encontram no mesmo nível de hierarquia, comunicando directamente uns com os outros e as aplicações possuem requisitos similares de fluxo. O modelo *peer-to-peer* é utilizado por defeito, quando não se tem qualquer informação acerca dos requisitos dos fluxos na rede, nem é possível determiná-los. Um exemplo de sistema com comportamento *peer-to-peer* é o acesso remoto.

O modelo de fluxos Cliente-Servidor é actualmente o mais aplicado. Este fornece informação de direcionalidade e hierarquia, sendo que os fluxos ocorrem nos dois sentidos na forma de pedidos e resposta entre clientes e servidor. Os fluxos são assimétricos porque exigem mais capacidade no sentido servidor cliente (resposta/ *downstream*) do que no sentido cliente servidor (pedidos/ *upstream*). Um exemplo de fluxo cliente-servidor é o serviço Web.

À medida que o modelo do fluxo cliente-servidor se torna mais hierárquico o seu comportamento pode ser representado como modelo de fluxo Cliente-Servidor Hierárquico. Neste modelo tem-se em conta os fluxos servidor-servidor e estes podem ser considerados fontes ou destinos de dados.

O modelo de fluxo de Computação Distribuída é o mais especializado dos modelos de fluxos. Este modelo pode ter o inverso das características de um modelo de fluxo cliente-servidor ou ser um híbrido dos modelos de fluxos *peer-to-peer* e cliente-servidor. Neste modelo, os fluxos podem ser primariamente entre um gestor de tarefas e os seus dispositivos de computação (tal como o modelo cliente-servidor), ou entre dispositivos de computação (tal como no modelo *peer-to-peer*). Este modelo é similar ao cliente-servidor, mas enquanto no modelo cliente-servidor os maiores fluxos são do servidor para o cliente, neste modelo os maiores fluxos são dos clientes para o servidor. A Figura 8 apresenta a configuração de cada um dos modelos de fluxos

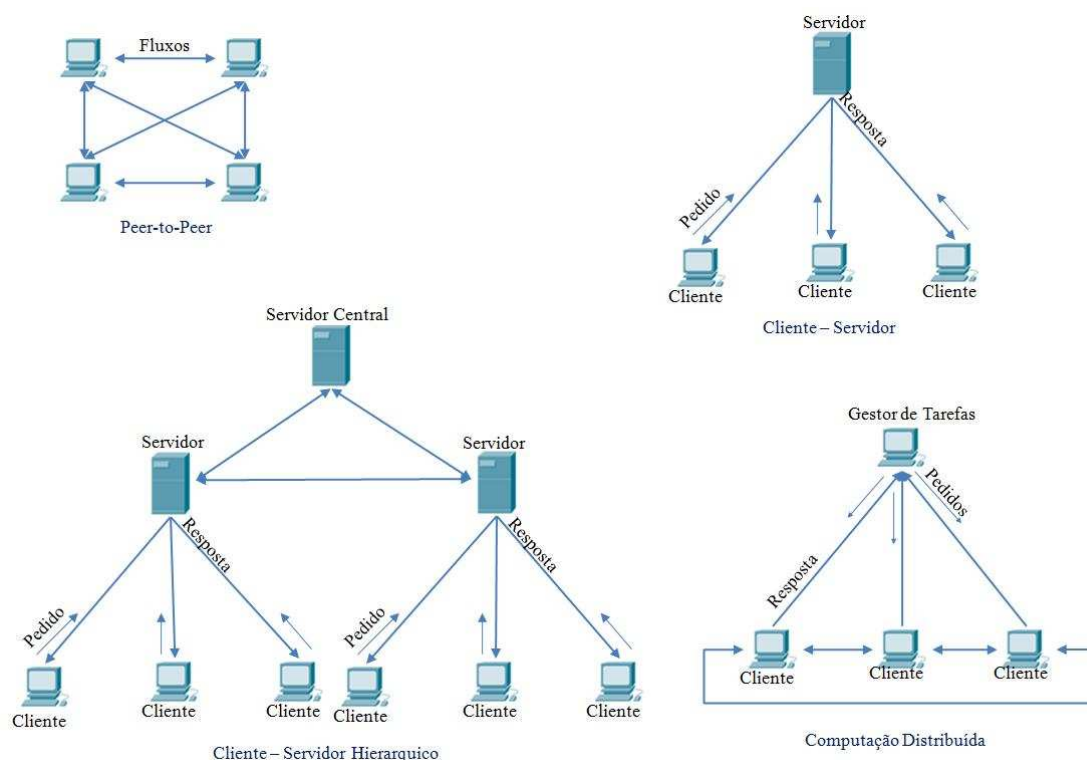


Figura 8. - Exemplos de Modelos de Fluxos

2.2.3 QoS dos Fluxos Individuais

O controlo de tráfego assegura que os recursos da rede sejam divididos de forma eficiente, de tal forma a maximizar o uso destes recursos enquanto assegura o cumprimento da QoS para os utilizadores. Portanto, neste contexto, os fluxos devem estabelecer contratos com a rede de maneira a limitar, em algum sentido, a quantidade de tráfego que os mesmos irão injectar na rede em determinado intervalo de tempo. O estabelecimento e manutenção destes contratos são pontos importantes para a garantia de fornecimento de serviço por parte da rede.

2.2.3.1 Caracterização do Débito

A identificação do tamanho médio dos blocos/pacotes de informação em situações de funcionamento normal e de excepção, caracterizará os valores de débito para as aplicações *Best-effort* e Adaptativas. A Tabela 4 mostra alguns exemplos de caracterização de fluxos de aplicações de *Best-effort* utilizadas em ambiente LAN e através da Internet. As estimativas destes valores foram baseadas em [1] e [2].

Tabela 4. – Exemplos de Fluxos do tipo *Best-effort*

Aplicação	Tempo de resposta óptimo [s]	Tempo de resposta tolerável [s]	Tamanho de dados normal [kB]	Tamanho de dados grande [kB]	Débito Nominal [kbit/s]	Débito Excepção [kbit/s]
Consulta Email	10	60	2	2000	2	533
Transacção WWW	5	30	10	500	16	133
Transacção Base Dados	1	6	1	100	8	133
Interacção remota	0,2	1	0,01	1	0,4	8
Transf. Ficheiros LAN	5	30	100	30000	160	8000
Transf. Fich. Internet	20	700	100	10000	40	114

Sabendo que o débito nominal é o débito mínimo necessário para realizar a transacção dentro do tempo de resposta óptimo, em situação de funcionamento normal (Blocos de tamanho normal). Este foi cálculo com base na fórmula (1).

$$\text{Débito Nominal} = \frac{\text{Tamanho de dados normal [bits]}}{\text{Tempo de resposta óptimo [s]}} \quad (1)$$

E tendo em conta que o débito de excepção é o débito mínimo necessário para realizar a transacção dentro do tempo de resposta tolerável, em situação de funcionamento de excepção (bloco de tamanho grande), utilizando para esta cálculo a fórmula (2).

$$\text{Débito de Excepção} = \frac{\text{Tamanho de dados grande [bits]}}{\text{Tempo de resposta tolerável [s]}} \quad (2)$$

Assim, o somatório do débito nominal indica as necessidades nominais de cada utilizador, obtidas em regime de utilização plena e simultânea das aplicações de comunicação que a infra-estrutura lhe disponibiliza.

A Tabela 5 mostra um resumo de alguns parâmetros típicos de funcionamento de aplicações adaptativas de transmissão de voz (VoIP) e de videoconferência (VCoIP) sobre redes IP, tendo em conta que os valores dos débitos são já a contar com a compressão dos dados. Os valores apresentados na Tabela 5 são extraídos de [2].

Tabela 5. – Exemplos de Fluxos de Áudio e Vídeo Adaptativos

Aplicação	Codificação	Débito Mínimo [kbit/s]	Débito Nominal [kbit/s]
VoIP	H.323	8	32
VCoIP	H.320 (MPEG 4)	32	64

2.2.3.2 Caracterização do Atraso

Para além dos débitos devem ser estimados valores máximos para o atraso máximo de *round-trip* das aplicações *Best-effort* e Adaptativas. Segundo [2], na determinação do valor do tempo de *round-trip* é considerado um factor de 0,1

relativamente ao tempo de resposta em funcionamento nominal ($t_{r.o}$), e um factor de 0,5 para aplicações de interacção remota. Assim, para o cálculo do atraso máximo usamos a fórmula (3).

$$Atraso\ máximo_{round-trip} = a * t_{r.o} \begin{cases} a = 0,1 \\ a = 0,5 \end{cases} \quad (3)$$

2.2.3.3 Caracterização das Perdas

As aplicações *Best-effort* são tolerantes às perdas. Neste tipo de aplicação as perdas são ultrapassadas através da retransmissão dos pacotes perdidos, o que se traduz em perda de eficiência e em aumento do atraso médio de *round-trip*. As aplicações Adaptativas são relativamente tolerantes às perdas. Nestas aplicações, a perda de pacotes é ultrapassada sem dificuldades de maior, resultando em degradação de qualidade devida à eliminação dos trechos de voz ou de vídeo, correspondentes à informação em falta.

2.2.4 Técnicas dos Fluxos Agregados

Os fluxos agregados são o resultado do somatório dos fluxos individuais que circulam nos vários pontos de uma estrutura de comunicações. São adoptados vários métodos para a caracterização dos fluxos agregados. Estes fluxos podem ser caracterizados usando o método Analítico ou utilizando Ferramentas de Simulação ou ainda através do dimensionamento das ligações.

O método Analítico utiliza modelos matemáticos para a caracterização dos fluxos agregados. São tradicionalmente utilizadas Distribuições de *Poisson*. O método de caracterização utilizando Ferramentas de Simulação é muito útil também na validação das opções de dimensionamento, pois permite a exploração de cenários alternativos e o estudo da sensibilidade do sistema de comunicação a parâmetros específicos de funcionamento. Da vasta gama de simuladores de redes disponíveis no mercado pode ser destacado aqui o *opnet* da *OPNET Technologies*.

O método do dimensionamento das ligações parte da caracterização das necessidades nominais e de excepção dos fluxos individuais e visa a obtenção de limites superiores para as necessidades dos agregados de fluxos, permitindo o dimensionamento das ligações para as situações limite de carga, correspondentes à utilização simultânea de uma determinada combinação de aplicações, estabelecida em função da quantidade e das características dos fluxos a montante da ligação a dimensionar.

2.2.5 Medições de Fluxos

Segundo [9], os sistemas de medições podem ser classificados como passivos e activos. Sua descrição e exemplos podem ser observados na Tabela 6.

Tabela 6. – Classificação dos Sistemas de Medições de Fluxos de Tráfego

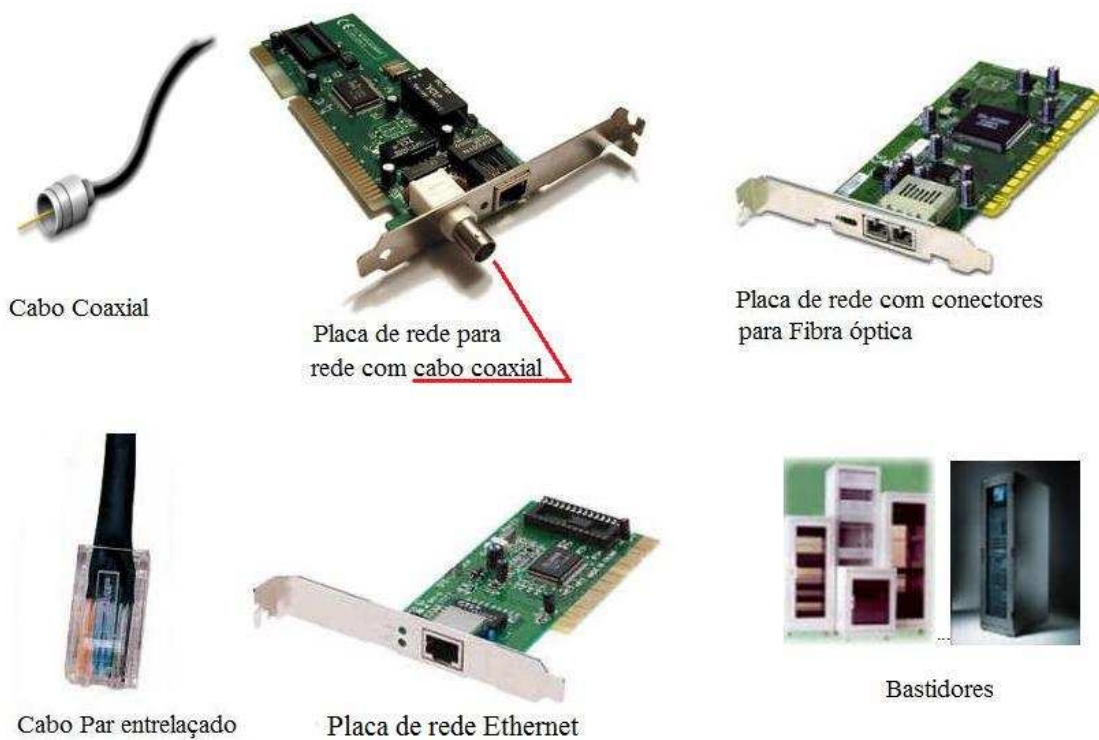
Sistemas	Descrição	Exemplos	Descrição
Activo	Injectam tráfego na rede e medem o seu desempenho baseado no que foi injectado	<i>Ping</i>	Fornece o tempo de <i>round-trip</i> de um pacote entre a origem e o destino
		<i>Traceroute</i>	Indica quais são os caminhos que um pacote percorreu até atingir o seu destino
Passivo	Observam o tráfego passando pelos pontos seleccionados dentro da rede. A recolha dos dados não afecta de forma significativa o tráfego que passa pela rede.	SNMP	Protocolo que permite efectuar medições de fluxos localizados nos interfaces dos routers e switches, aplicando algumas métricas específicas dos fluxos
		Simuladores de tráfego	Ferramentas de monitorização de redes, como por exemplo o Cisco IOS <i>NetFlow</i>

Segundo [10], para os fluxos do tipo *Best-effort* não é possível especificar fiabilidade ou requisitos de atraso, só a capacidade será considerada nos cálculos. Para os fluxos especificados todas as suas características devem ser usadas nos cálculos. Quando o atraso ou a fiabilidade garantida fazem parte dos requisitos estes serão usados individualmente nos cálculos.

2.3 Equipamentos de Rede

Para montar uma rede precisamos de dispositivos que nos permitem construir as redes. Existem três tipos de equipamentos de rede: os Passivos, Activos e Finais. Nos equipamentos Passivos encontram-se os cabos coaxiais, de par entrançado e

de fibra óptica, os conectores e tomadas, painéis de interligação (*patch panel*) e bastidores. Dos Activos fazem parte os switches e os routers. Nos equipamentos Finais encontramos os dispositivos de apoio ao utilizador como os PCs e servidores. Na Figura 9 estão exemplificados estes tipos de equipamentos.



Equipamento Passivo



Equipamento Activo



Figura 9. – Exemplos de equipamentos

2.4 Resumo

Este capítulo descreve o estado da arte associado ao projecto de redes. Foi dividido em quatro secções. Na primeira secção foi efectuada uma análise das redes de comunicações em geral comparando a rede a um conjunto de sistemas ligados entre si, incluindo utilizadores, aplicações, dispositivos e equipamentos da rede. Na segunda secção, descreve-se a forma como a rede de dados se relaciona em termos de hierarquia e diversidade. Na terceira secção efectua-se uma análise dos requisitos do sistema, incluindo os requisitos de utilizador, aplicações e dispositivos. Finalmente, na quarta secção, descreve-se a análise de fluxos, tendo em conta os tipos e os modelos de fluxos que podem ser encontrados.

3 Projecto da Rede

Para criação da rede do ISCED foi necessário efectuar um levantamento de requisitos que permitiu saber quais as necessidades básicas desta instituição. Foi necessário analisar o funcionamento da instituição e de seguida prosseguir com a elaboração da rede de acordo com as necessidades da mesma.

3.1 Levantamento de Requisitos

3.1.1 Utilizador

Nem todos os serviços a disponibilizar pela rede serão usufruídos por todos os utilizadores da rede. Haverá serviços que serão disponibilizados apenas para utilizadores concretos da área administrativa, como por exemplo serviços de gestão de pessoal.

Foram identificados sete grupos de utilizadores que desempenham um papel activo dentro da instituição. Estes grupos de utilizadores, apresentados na Tabela 7, têm necessidades comuns em termos de rede de dados, como por exemplo a consulta de email, partilha de ficheiros, correio electrónico, acesso à Internet e outras.

Tabela 7. – Grupos de Utilizadores

Grupo	Nome	Descrição
G1	Presidência e a Direcção	Presidente, Director e todos os funcionários que trabalham directamente com eles, tais como assessores e secretários
G2	Funcionários da contabilidade e finanças e recursos humanos	Funcionários da secção da Contabilidade e Finanças, e da secção dos Recursos Humanos
G3	Funcionários do secretariado e dos assuntos académicos	Funcionários ligados ao Secretariado geral e aos departamentos de Assuntos Académicos que tratam da documentação dos estudantes desde a candidatura até à finalização do curso
G4	Funcionários do património	Funcionários que tratam da logística da instituição. São os responsáveis pelo aprovisionamento
G5	Funcionários Administrativos	Grupo de todos os outros funcionários da instituição excluindo os docentes, contabilidade, secretariado.
G6	Docentes	Professores da instituição
G7	Estudantes	Alunos da instituição que se encontram correntemente inscritos

A Instituição prevê para um futuro próximo de construção de mais uma sala de informática e um laboratório de redes informáticas. Em termos de número de utilizadores há previsão de aumento de 4% para os estudantes, 8% de Docentes e 13% de Administrativos no decorrer deste ano lectivo, o que totaliza um crescimento aproximadamente de 5% de utilizadores

3.1.2 Aplicações

O levantamento das aplicações foi feito tendo em conta a perspectiva dos utilizadores em relação à rede na instituição. As aplicações desejadas foram as dos serviços básicos das redes locais tradicionais, tais como email, Web e transferência de ficheiros. Também são necessárias algumas aplicações de gestão empresarial para alguns utilizadores de modo a melhor gerir a instituição.

Algumas aplicações, tais como o email, existem em todo o lado, para toda a gente usar e deverão estar disponíveis em quase todos os dispositivos (exemplo: servidores, *desktops* e *laptops*). No entanto, existem aplicações tais como as aplicações de gestão financeira, que são usadas apenas por determinados grupos de utilizadores.

Para que existam diversos serviços de comunicação como a transferência de ficheiros, a troca de correio electrónico, o acesso remoto, a troca de informações Web, a gestão de rede entre outros, será necessário que haja um conjunto de aplicações ou protocolos de suporte. Os serviços de utilizador final (email, Web e transferência de ficheiros) e os serviços de suporte (DHCP, DNS, NAT e Gestão), bem como uma descrição dos seus respectivos protocolos.

O email é um serviço de correio electrónico que utiliza os protocolos SMTP, POP e IMAP. O protocolo SMTP é utilizado para o envio das mensagens do cliente para o servidor. Os protocolos POP e IMAP são utilizados para aceder às mensagens localizadas no servidor e trazê-las para o cliente. A diferença entre o POP e o IMAP é que este último pode transferir apenas parte da mensagem.

O serviço Web é um serviço que permite visualizar páginas de Internet. Este serviço utiliza o protocolo HTTP para transferir os conteúdos das páginas.

Para efectuar transferências de ficheiros utiliza-se principalmente o protocolo FTP. Este permite receber ou enviar ficheiros de e para um computador remoto, assim como fazer a gestão dos directórios e ficheiros pertencentes ao utilizador.

O serviço DHCP utiliza o protocolo DHCP. Este protocolo é usado para atribuir automaticamente endereços lógicos aos dispositivos da rede. Todos os dispositivos ligados à rede TCP/IP têm que ser configurados com um endereço IP. O administrador da rede pode atribuir manualmente os endereços aos dispositivos ou usar um servidor DHCP para atribuir endereços dinamicamente. O DHCP distribui automaticamente os endereços IP, máscaras, IP do *default gateway* da rede e outras configurações para os computadores da rede.

O DNS é um mecanismo de resolução de nomes em endereço IP. O objectivo é facilitar a identificação dos dispositivos da rede a partir de um nome legível pelos humanos, num endereço IP legível pelas máquinas. Os nomes e endereços IP são armazenados em tabelas de bases de dados que ficam armazenados nos servidores DNS.

O NAT tem a função de traduzir os endereços válidos e registados de acesso à Internet para os endereços reservados da rede interna e vice-versa. O NAT pode

ser implementado num router ou numa Firewall. O router com NAT monta uma tabela com um endereço local interno e um endereço externo. Assim, a rede interna com endereços privados pode aceder a endereços IP públicos da rede Internet.

Os serviços de Gestão são serviços que permitem gerir a rede e que para esse efeito utilizam o protocolo SNMP, que é um protocolo de troca de informação de gestão entre dispositivos. Este protocolo é implementado de acordo com uma arquitectura cliente-servidor, em que o cliente é o gestor de rede e o servidor é um agente. O agente contém toda a informação de gestão relacionada com o objecto gerido numa base de dados denominada MIB. Para aceder à informação de gestão do agente, o gestor utiliza o protocolo SNMP.

Para além dos serviços descritos acima, por necessidade da instituição, a rede a instalar deverá estar preparada para suportar serviços de integração de voz na rede (VoIP) bem com de videoconferência. Por isso, foi tido em conta os recursos que estas aplicações necessitam da rede de modo a garantir a qualidade de serviço para o bom funcionamento da rede.

A instituição necessita de mecanismos que lhe irão permitir organizar, estruturar e controlar todas as suas actividades quer a nível de estudantes quer a nível organizacional e para isso utilizará aplicações de gestão que lhe permitirão alcançar esses objectivos. Sendo essas aplicações de gestão de estudantes, de stocks, financeira e de pessoal. Na Tabela 8 podemos observar os grupos de utilizadores da instituição segundo as suas necessidades

Tabela 8. – Grupo de Utilizadores por Necessidade de Aplicação

Aplicação	Utilizadores
WEB, Email, Partilha de Ficheiros e VCoIP e VoIP	Presidência e Direcção
	Funcionários administrativos
	Funcionários do secretariado e assuntos académicos
	Funcionários do Património
	Funcionários da contabilidade e finanças
	Docentes
	Estudantes
Aplicações de Gestão de Estudantes	Funcionários do secretariado e assuntos académicos
Aplicações de Gestão de Stocks	Funcionários do Património
Aplicações de Gestão Financeira	Presidência e Direcção
	Funcionários da contabilidade e finanças
Aplicações de Gestão do Pessoal	Presidência e Direcção

3.1.3 Dispositivos

Os dispositivos são normalmente descritos por alguns parâmetros tais como, capacidade de armazenamento (disco rígido) e processamento (processador), quantidade de RAM, placa gráfica, eficiência energética e velocidade de resposta global do dispositivo (latência de interactividade). Destes parâmetros foram escolhidos os apresentados na Tabela 9, na qual se indicam os requisitos que os dispositivos necessitam de possuir para garantir uma boa execução de uma aplicação específica.

Nessa Tabela, são usadas as opções “Alto” (A), “Médio”(M) e “Baixo”(B) para classificar os parâmetros. A opção “Alto” define que a aplicação requer um valor mais alto deste requisito para este dispositivo, a opção “Baixo” define que a aplicação requer um valor mais baixo deste requisito para este dispositivo e a opção “Médio” indica um valor intermédio.

Tabela 9. – Requisitos dos Dispositivos por Aplicação

Aplicação	Requisitos				Dispositivo
	Armazenamento (Disco rígido)	Processamento	Latência	RAM	
Email	A	B	M	B	PC ou Servidor
FTP	A	B	M	B	PC ou Servidor
Web	M	M	B	M	PC ou Servidor
BD	A	A	B	A	Servidor BD
Gestão Financeira	B	B	M	B	PC
Gestão de Stocks	B	B	M	B	PC
Gestão do Pessoal	B	B	M	B	PC
Gestão de Estudantes	B	B	M	B	PC

Na Tabela 9, pode-se reparar que os requisitos referidos como necessários para os serviços de gestão (gestão financeira, de stocks, do pessoal e de estudantes) para o utilizador são bastante menores do que os presumíveis para aplicações de gestão. Isto deve-se ao facto dos serviços de gestão serem suportados pelos serviços de BD e por, esse motivo, os serviços de gestão da Tabela 9 são relativos à interface com o utilizador.

3.1.4 Rede

A rede de dados a instalar tem um total de 6205 utilizadores, sendo 6021 estudantes, 136 Docentes e 48 Funcionários Administrativos repartidos pelos três edifícios do *campus*. Grande parte destes utilizadores estão concentrados no edifício principal, estando os restantes distribuídos pelos outros dois edifícios. Sendo assim a rede a ser implementada deverá cobrir toda a área ocupada do ISCED, suportar o número actual de utilizadores bem como uma boa capacidade para futura expansão.

Esta rede deverá ser robusta de forma a reduzir os tempos de inoperacionalidade. Deverá disponibilizar serviços de troca de dados, partilha de impressoras e correio electrónico entre outros. A rede deverá estar preparada para suportar a utilização de tecnologias de rede sem fios, bem como, suportar serviços de VCoIP, e VoIP. Por fim deverá ser implementadas medidas de segurança na rede e possuir capacidades de gestão de forma autónoma.

3.1.4.1 Definição dos Locais a Abranger pela Rede

Como já foi dito anteriormente, o ISCED é constituído por 3 edifícios. Dois dos edifícios são compostos por três pisos e o terceiro por apenas um piso. A rede a instalar deverá abranger os três edifícios dos ISCED. Na Figura 10, podemos observar os edifícios e as suas respectivas localizações

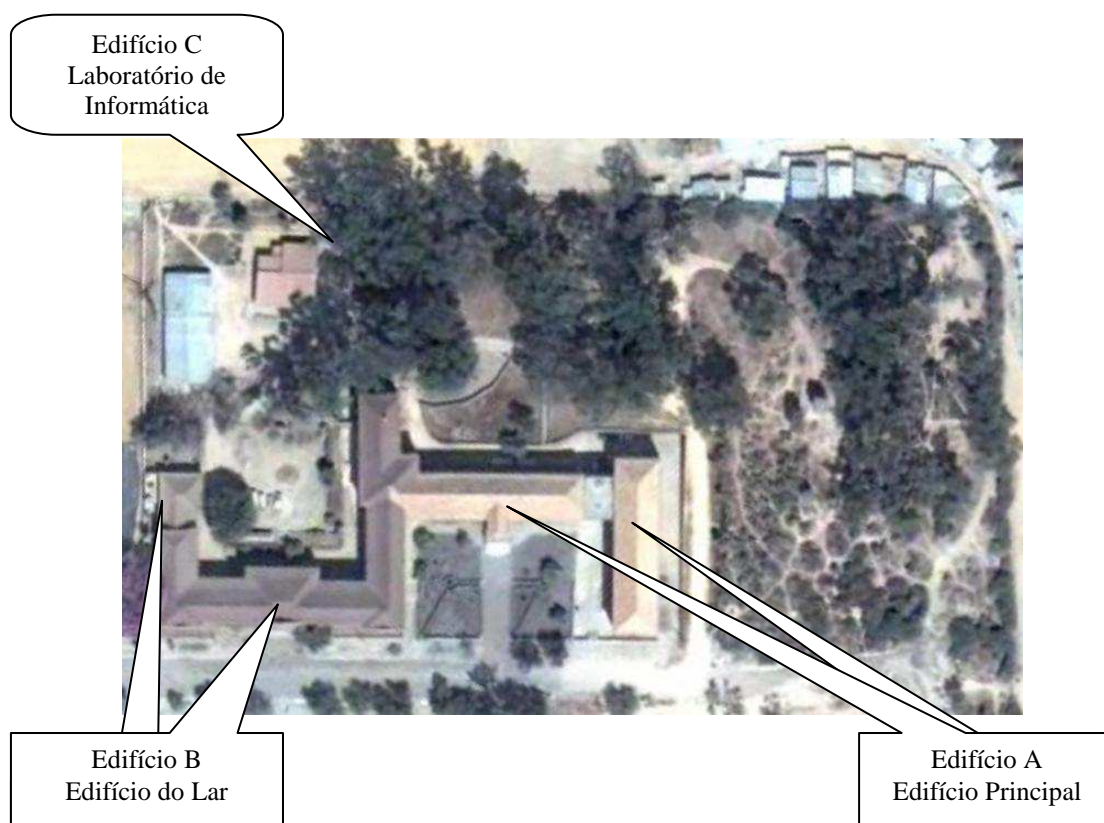


Figura 10. – Vista aérea do ISCED

3.1.4.2 Definição da Topologia da Rede

Na Figura 11, podemos ver de forma generalizada como a rede estará interligada. A captação do sinal Internet será feita por satélite e será distribuído para os três edifícios da instituição que por sua vez terão diferentes pontos de acesso.

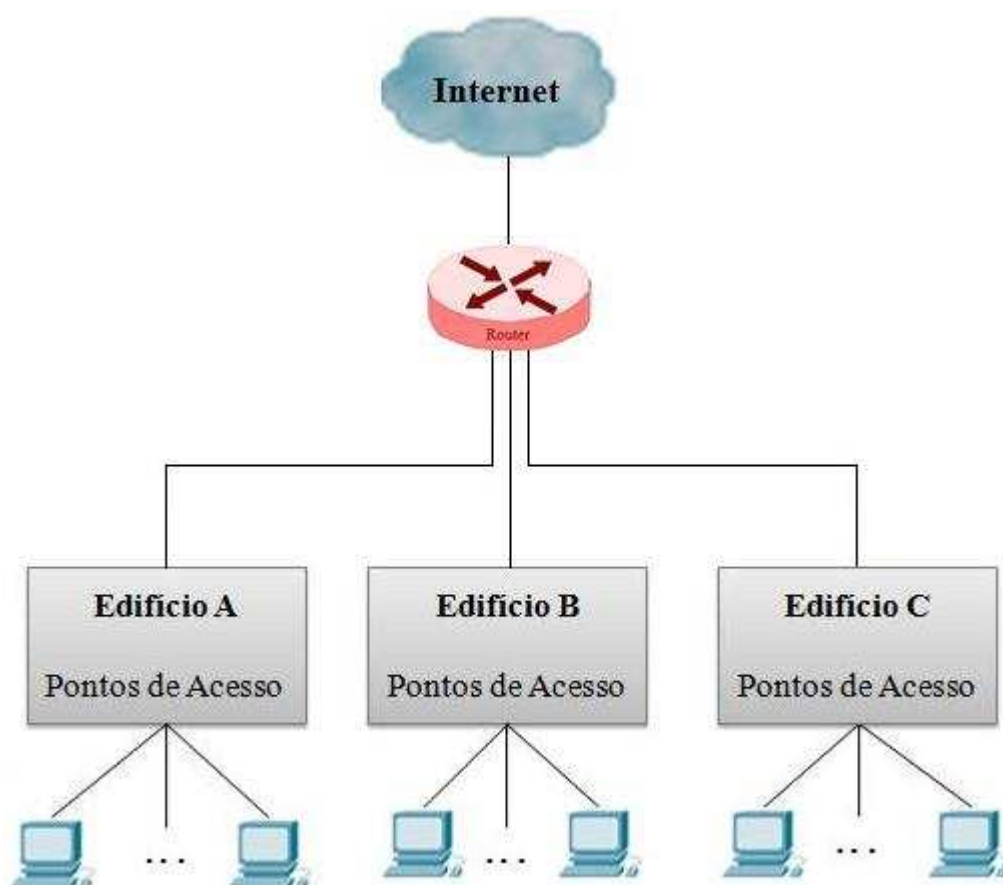


Figura 11. – Modelo Geral da Interligação da Rede

3.1.4.3 Redundância

Para o sistema deste projecto, como se trata de uma instituição de ensino, decidiu-se que era necessário um *uptime* de 99,999% que segundo [1], corresponde a ter um *downtime* inferior a 5,3 minutos por ano ou 86ms por dia. Normalmente, o *uptime* é medido ponto-a-ponto quer entre dispositivos de utilizadores (dispositivos de computação genéricos) ou entre equipamentos de rede (router e switches). O *uptime* pode ser medido em termos de falta de conectividade ou como uma taxa de perdas (taxa de erros de bit/célula/trama, taxa de perda de pacotes). Para verificar e testar a conectividade da rede pode ser utilizado o *ping*.

Durante o levantamento de requisitos deve-se ter em conta a existência de um *downtime* calendarizado para futuros *upgrades* de *hardware* e *software*, reconfiguração da rede ou correr testes. Esse *downtime* não deve contar para o *downtime* global da rede e deve ser incluído nos requisitos de desempenho.

Por causa de como, onde e quando é medido o *uptime* poderá haver diferentes requisitos de *uptime* para diferentes partes da rede, a que se refere o *uptime*. Por exemplo, pode haver um requisito geral para a rede toda medido em qualquer lugar, ou outro requisito de alto desempenho medido apenas entre dispositivos (servidores) e equipamentos (router/switch) vitais da rede.

É necessário assegurar a redundância na topologia. Quer redundância a nível de servidores, router e switches quer ao nível das ligações. Deverá ser aplicada, ao sistema, redundância física e redundância lógica, de modo a alcançar um *uptime* de 99,999% nos servidores e no router/switch CORE.

3.1.4.4 Definição dos Locais das Aplicações por Edifício

Para o caso referido neste trabalho, pode-se ver na Figura 12 o mapa das aplicações localizadas dentro dos pisos de cada edifício que compõe o ISCED. Na Figura 12, pode-se observar as aplicações existentes em cada andar do respectivo edifício. Sendo que o edifício A é o que tem maior necessidade de recursos em termos de aplicações produzindo assim um maior tráfego de dados.

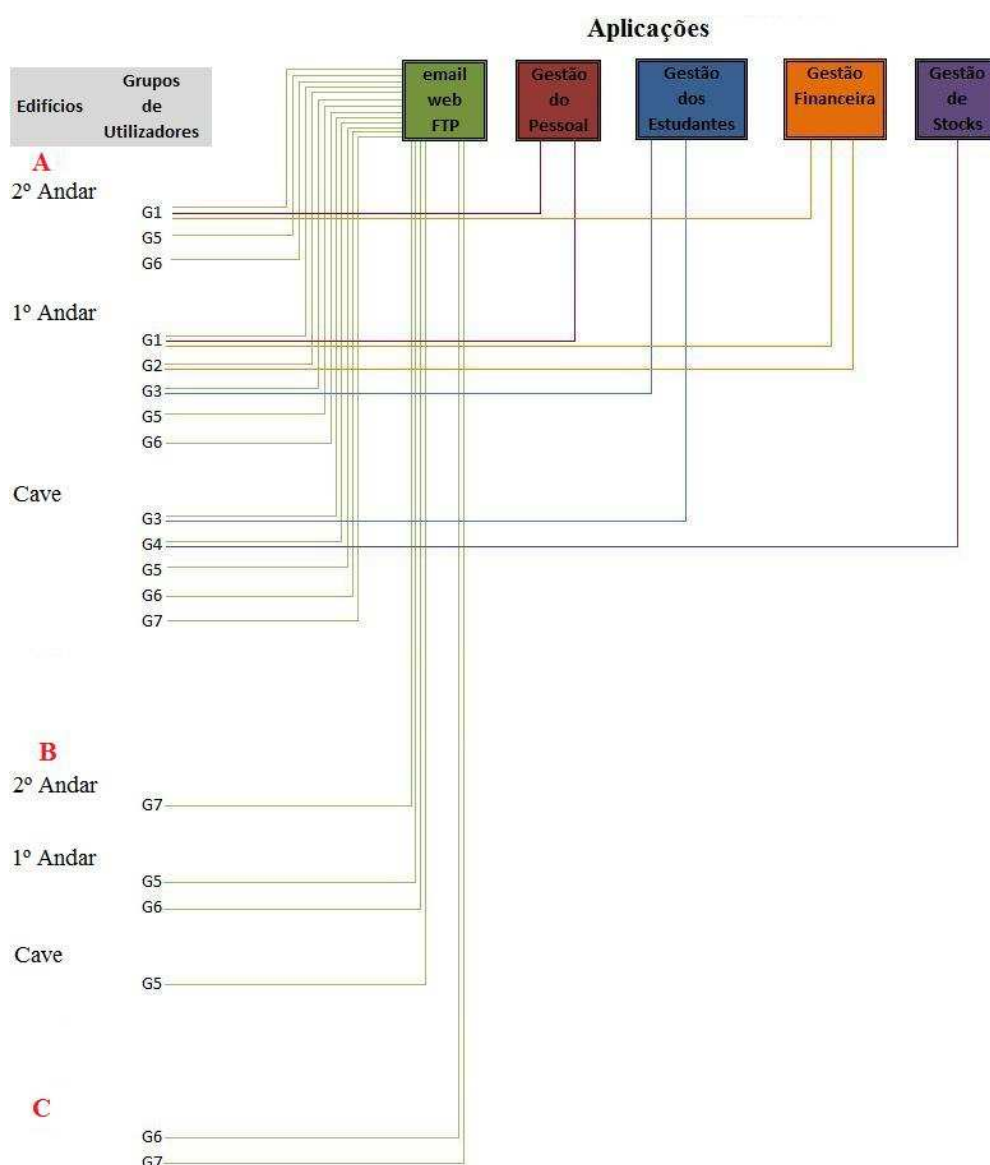


Figura 12. – Locais das Aplicações

Para que haja sempre disponibilidade da rede é necessário que o tráfego gerado pelo edifício A seja separado do tráfego gerado nos restantes edifícios. Para garantir que não haja dependências entre edifícios devemos criar subredes para cada edifício. As subredes possibilitam a separação física do tráfego gerado em cada edifício.

Também pode ser visto na Figura 12, que há grupos de utilizadores com mais necessidade de recursos da rede que outros, como é o caso dos grupos que precisam de outros tipos de aplicações para além do email, Web e FTP. Esses Grupos têm maior exigência da rede em termos de rapidez na interactividade entre cliente e servidor. A Tabela 10 indica a percentagem de utilização do serviço por tipo de aplicação, num total de 279 postos de trabalho.

Tabela 10. – Percentagem de Tráfego por Tipo de Aplicação

Aplicação	Grupo de utilizadores	Postos de Trabalho	Utilização de Serviço
Email, Web e FTP	G1, 2, 3, 4, 5, 6 e 7	279	100,00%
Gestão do pessoal	G1	3	1,08%
Gestão financeira	G2	11	3,94%
Gestão de estudantes	G3	17	6,09%
Gestão de stocks	G4	2	0,72%

Tendo em conta o crescimento previsto na rede e a imprecisão dos números foi feito um arredondamento por excesso para o número inteiro mais próximo para melhor compreensão. Sendo assim, pode-se dizer que o tráfego da rede para a aplicação de gestão do pessoal será aproximadamente de 2%, para gestão de

estudantes será de 7%, para gestão financeira de 4% e para a gestão de stocks de 1%.

Dentro dos grupos de utilizadores haverá grupos que terão restrições em determinadas aplicações, tais como o grupo dos estudantes. O grupo dos estudantes terá acesso livre ao email e terá restrições relativamente à Web e à partilha de ficheiro, tendo acesso neste último apenas a documentação disponibilizada para o estudante.

O grupo da presidência e da direcção terá permissões de tudo, e toda a documentação gerada por eles deverá ser transmitida na rede de forma segura e confidencial. O grupo da contabilidade e finanças que engloba os recursos humanos deverá ter acesso à base de dados da secretaria e assuntos académicos e a base de dados do património de forma unidireccional.

Este trabalho propõe um modelo hierárquico para o projecto tal como já foi especificado anteriormente. O modelo de funcionamento desta rede foi obtido através da análise de requisitos das aplicações. O estabelecimento deste modelo tem por objectivo a definição para cada grupo de utilizadores, das aplicações a suportar e das arquitecturas protocolares (exemplo: TCP/IP) necessárias ao suporte das aplicações. Assim primeiramente fez-se a caracterização dos grupos de utilizadores em função da sua dimensão, da sua localização na infra-estrutura e dos serviços de comunicação utilizados.

Nesta caracterização foram considerados todos os grupos de utilizadores que fazem parte da estrutura de rede para efectuar trocas de informações dentro da instituição e com o exterior desta, através de outros sistemas de comunicações. A Tabela 11 indica as aplicações em cada edifício da instituição e mostra o número de grupo de utilizadores que irão usufruir dessas respectivas aplicações. Todas as

aplicações descritas assentam na arquitectura protocolar TCP/IP. Para estas aplicações o tipo de tráfego é *Best-effort* à excepção das aplicações de VoIP e VCoIP cujo tráfego é *Continuous-media*.

Tabela 11. – Caracterização dos Grupos de Utilizadores

Edifício	Aplicação	Grupo	Nº Utilizadores
A	Email	G1, G2, G3, G4, G5, G6, G7	157
	Web	G1, G2, G3, G4, G5, G6, G7	157
	Partilha de Ficheiros	G1, G2, G3, G4, G5, G6, G7	157
	Gestão de Pessoal	G1	3
	Gestão Financeira	G1, G2	11
	Gestão de Estudantes	G3	17
	Gestão de Stocks	G4	2
	Base de Dados	G1, G2, G3, G4	33
B	Email	G5, G6, G7	49
	Web	G5, G6, G7	49
	Partilha de Ficheiros	G5, G6, G7	49
C	Email	G6, G7	73
	Web	G6, G7	73
	Partilha de Ficheiros	G6, G7	73

3.1.4.5 Restrições da rede

Em termos de instalação de cablagem, deverá ter-se em conta a estrutura antiga do edifício. Deverão ser vistas as condicionantes a nível de integração de novas arquitecturas protocolares, uma vez que a instituição já tem uma rede instalada. A estrutura de rede a instalar deverá ter capacidade de crescimento até 50% sem necessidade de qualquer alteração, bem como estar preparada para suportar comunicações multimédia e maiores volumes de tráfego.

Os bastidores deverão ser colocados num local arejado e acessível, e a sua régua de tomadas deverá ser ligada a uma UPS que se ligará por sua vez à rede de energia do ISCED. Os cabos deverão ficar isolados de cabos de energia. Os cabos UTP deverão ser instalados em esteira, calha metálica ou calha de rodapé. No distribuidor-bastidor deverá ser feita a ligação do tensor metálico e das blindagens envolventes do cabo a contactos de terra existentes nos "*patch panels*".

Os cabos deverão ser ainda identificados de forma clara e indelével com o número da tomada a que correspondem nas extremidades. As tomadas RJ45 devem ser instaladas em caixas embutidas na parede ou em caixas de pavimento consoante as necessidades. Deverão ser numeradas com um número sequencial correspondente à sua localização nos painéis passivos do bastidor. Após a realização da obra deverão ser efectuados testes e ensaios a todo o equipamento.

3.2 Topologia do ISCED

O ISCED tem uma área bruta que ronda cerca de 2 hectares e é composto por 3 edifícios; um edifício principal (A) com 3 pisos, onde funciona a grande parte administrativa e algumas salas de aulas; um outro edifício do Lar (B) também com 3 pisos onde funciona o Lar do Instituto com algumas salas de aulas e também uma pequena parte administrativa; um último edifício (C) com apenas 1 piso que contém 2 salas de informática e a repartição de informática. Este edifício é chamado de laboratório de informática.

As plantas do ISCED são referidas no Anexo A, onde podemos encontrar as plantas detalhadas para cada andar do edifício A. Os postos de trabalho encontram-se localizados nos três edifícios que compõem a instituição. Na Tabela 12 observa-se a quantidade de postos de trabalho permanentes previstos em cada andar dos três edifícios referidos.

Tabela 12. – Localização dos Postos de Trabalho

Edifício	Nº de Postos de Trabalho por grupo de utilizador		Total de Postos de Trabalho por Edifício
A			
2º Andar	Presidência	1	33
	Funcionários	5	
	Docentes	27	
1º Andar	Direcção	2	56
	Funcionários	25	
	Docentes	29	
Cave	Funcionários	7	68
	Docentes	44	
	Estudantes	17	
B			
2º Andar	Estudantes	10	10
1º Andar	Funcionários	6	
	Docentes	28	
Cave	Funcionários	5	5
C			
	Docentes	8	8
	Estudantes	65	

Tendo em conta o crescimento futuro da Instituição, os postos de trabalho previstos são indicados na Tabela 13.

Tabela 13. – Localização dos Postos de Trabalho Actuais e Futuros

Edifício		Postos de Trabalho Permanentes	Edifício		Postos de Trabalho Previstos
A		157	A		452
2º Andar	33		2º Andar	130	
1º Andar	56		1º Andar	172	
Cave	68		Cave	150	
B		49	B		80
2º Andar	10		2º Andar	20	
1º Andar	34		1º Andar	40	
Cave	5		Cave	20	
C		73	C		80
	73			80	

3.3 Dimensionamento

Neste capítulo é analisado, o modelo de funcionamento da rede e feito o dimensionamento do débito das ligações para rede local e Internet. O dimensionamento é o processo onde se determina a configuração física da rede para que esta suporte os fluxos de tráfego previstos e com um custo de rede mínimo.

3.3.1 Especificação dos Fluxos

A estimativa da caracterização dos fluxos e o dimensionamento das ligações foram feitas tendo em conta o crescimento futuro da instituição. Neste projecto procura-se mostrar que é importante a análise de fluxos do tráfego, numa fase inicial, para escolher melhor a tecnologia e equipamentos a utilizar, e para numa fase posterior, monitorar a rede e verificar as suas falhas. Neste projecto, o edifício A é o que terá maior tráfego e por isso maior impacto sobre a arquitectura da rede. É feita a análise dos fluxos que passam neste edifício.

São identificadas três fronteiras de fluxos no nosso modelo hierárquico da rede. A primeira fronteira é entre os postos de trabalho e a camada de acesso, a segunda fronteira é entre a camada de acesso e a camada de distribuição e a última fronteira é entre a camada de distribuição e o CORE. A Figura 13 apresenta essas fronteiras e indica os tipos de fluxos que atravessam cada fronteira. FI representa os Fluxos Individuais em cada posto de trabalho e FA representa os Fluxos Agregados.

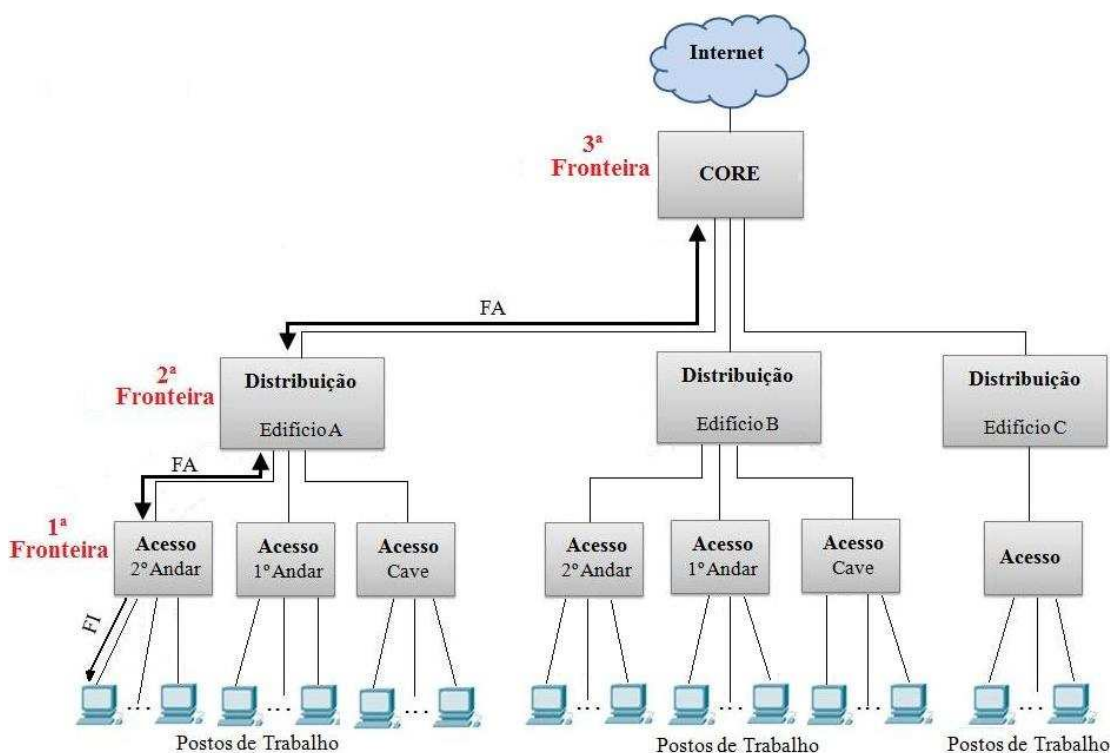


Figura 13. – Fronteiras dos Fluxos e seus respectivos Tipos de Fluxos

Para melhor efectuar os cálculos dos fluxos da rede, os fluxos individuais foram agrupados tendo em conta as necessidades de cada grupo de utilizadores, ou seja, como todos os grupos de utilizadores têm a mesma necessidade em termos de email, Web, FTP e Internet então foi criado um grupo de fluxos individuais chamado FI Comum. Foi também criado um fluxo individual para cada grupo de utilizadores, como é mostrado na Tabela 14. Os valores dos débitos para as aplicações de gestão foram relacionados com os valores das aplicações de transferência de ficheiros LAN estimados em [2].

Tabela 14. – Cálculo dos Fluxos da Rede

Grupo de utilizadores	Aplicação	Débito Nominal [kbit/s]	Grupo do FI	Total do débito do Grupo de FI [kbit/s]
G1, G2, G3, G4, G5, G6 e G7	Email	2	FI Comum	218
	Web	16		
	FTP	160		
	Internet	40		
G1	Gestão do Pessoal	160	FI G1	546
	Gestão Financeira	160		
	BD	8		
G2	Gestão Financeira	160	FI G2	386
	BD	8		
G3	Gestão de Estudantes	160	FI G3	386
	BD	8		
G4	Gestão de Stocks	160	FI G4	386
	BD	8		

A análise dos fluxos foi baseada nos seus modelos. A caracterização dos fluxos na primeira fronteira baseou-se no modelo cliente-servidor tendo em conta apenas os tipos de aplicações *Best-effort*. Na segunda e terceira fronteiras utilizou-se o modelo cliente-servidor hierárquico. A análise dos fluxos serviu para identificar os tipos de equipamentos de rede a utilizar em cada fronteira de modo a satisfazer os requisitos dos utilizadores. A Figura 14 caracteriza os fluxos da primeira e segunda fronteiras para o edifício A.

Na Figura 14 pode ser observado que a tecnologia Ethernet a utilizar entre a camada de acesso e a camada de distribuição é de 100Mbit/s. E para a ligação entre a camada de distribuição e a camada CORE, pode-se optar por utilizar uma tecnologia Ethernet 1Gbit/s.

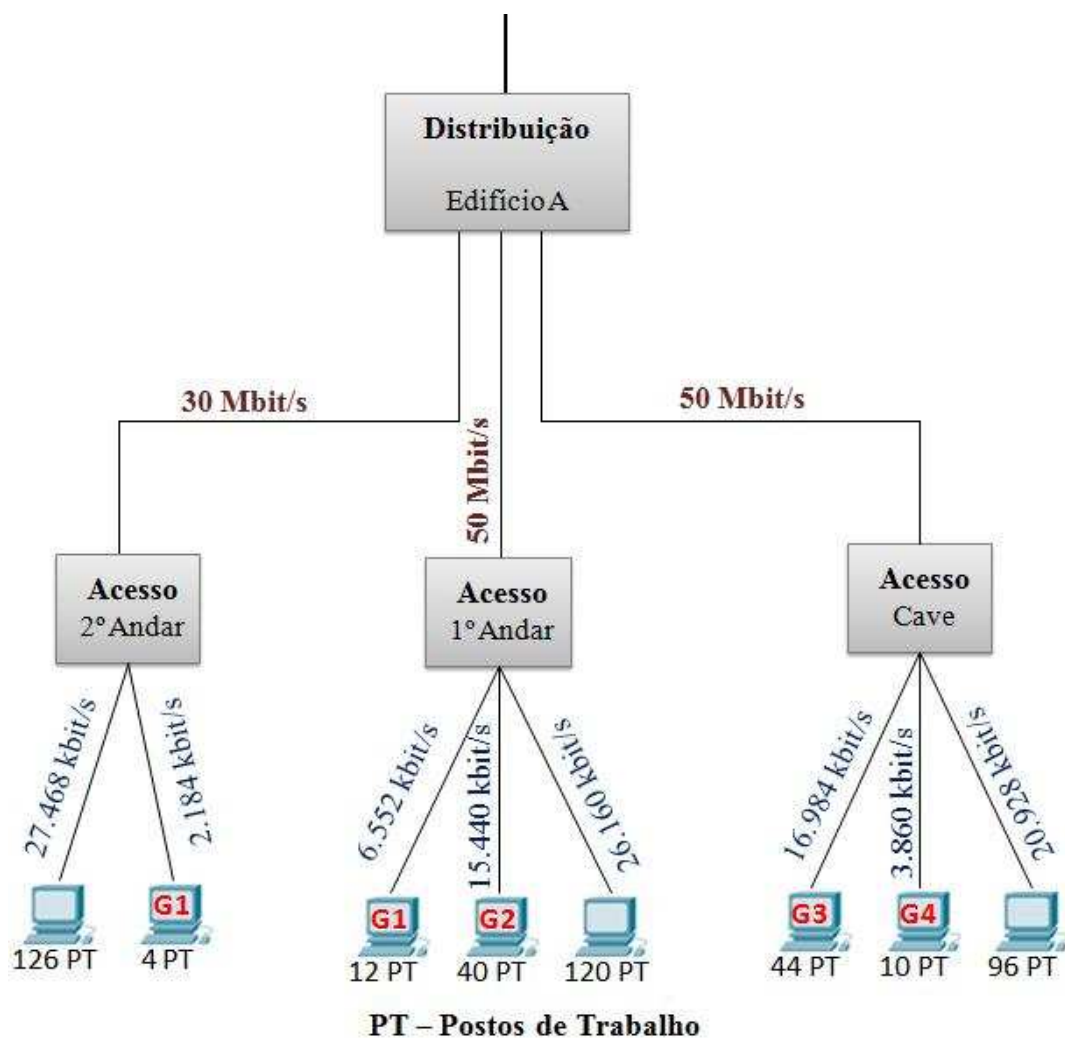


Figura 14. – Caracterização do Fluxo para a Primeira e Segunda Fronteiras

3.3.2 Ligações

É apresentado na Tabela 15 o dimensionamento das ligações LAN, sendo os valores calculados baseados nos descritos em [2]. Os cálculos foram efectuados relativamente ao edifício A, pois é o que tem mais utilizadores permanentes, assumindo valores semelhantes para os outros dois edifícios.

No dimensionamento das ligações LAN foram consideradas as aplicações identificadas na análise de requisitos. Tendo em conta a previsão de utilização futura e os cálculos dos fluxos estabelecidos para o edifício A, optou-se por um sobredimensionamento da capacidade das ligações de 1Gbit/s ao CORE o que produz uma taxa de utilização de aproximadamente 4%, como pode ser observado na Tabela 15.

Tabela 15. – Dimensionamento de Débito em ligações LAN

Aplicações	Débito Nominal [kbit/s]	Débito Excepção [kbit/s]	Fluxos a montante	Fluxos a jusante	Factor de simultaneidade	Débito Total p/ Aplicação [kbit/s]
Consulta Email	2	533	452	452	1	723
Transacção WWW	16	133	452	45,2	0,1	723
Transacção Base Dados	8	133	452	45,2	0,1	362
Interacção remota	0,4	8	452	452	1	181
Transf. Ficheiros LAN	160	8000	452	226	0,5	36160
Transf. Fich. Internet	40	114	452	45,2	0,1	1808
VoIP	32	64	452	45,2	0,1	1446
Necessidade total de Débito na ligação agregada [kbit/s]						41403
Capacidade mínima da ligação [kbit/s]						8000
Especificação de débito da ligação agregada [kbit/s]						1000000
Taxa nominal de utilização da ligação agregada [%]						4

3.4 Arquitectura Lógica da Rede

Na estrutura de rede a instalar foram considerados os três subsistemas. O primeiro é o CORE que tem a responsabilidade de efectuar o acesso tanto ao exterior (Internet) como ao interior (Subsistema de distribuição), através de equipamentos activos como routers e router/switch. O segundo subsistema, a camada de distribuição, irá permitir a comunicação entre o âmbito local e o CORE, através de routers e switches. Por fim o terceiro subsistema é a camada de acesso.

A função principal do subsistema de acesso é de interligar cada posto de trabalho com os bastidores de rede. A topologia física a adoptar será a estrela construída em cabo UTP desde o bastidor até as tomadas RJ-45 e em fibra óptica para interligar os bastidores secundários (B e C) ao bastidor principal (A). Pode ser observada na Figura 15 a arquitectura lógica da rede. Por uma questão de redundância, definiu-se uma topologia emalhada. Na Figura 19 pode ser observada a topologia emalhada que permitirá obter caminhos redundantes.

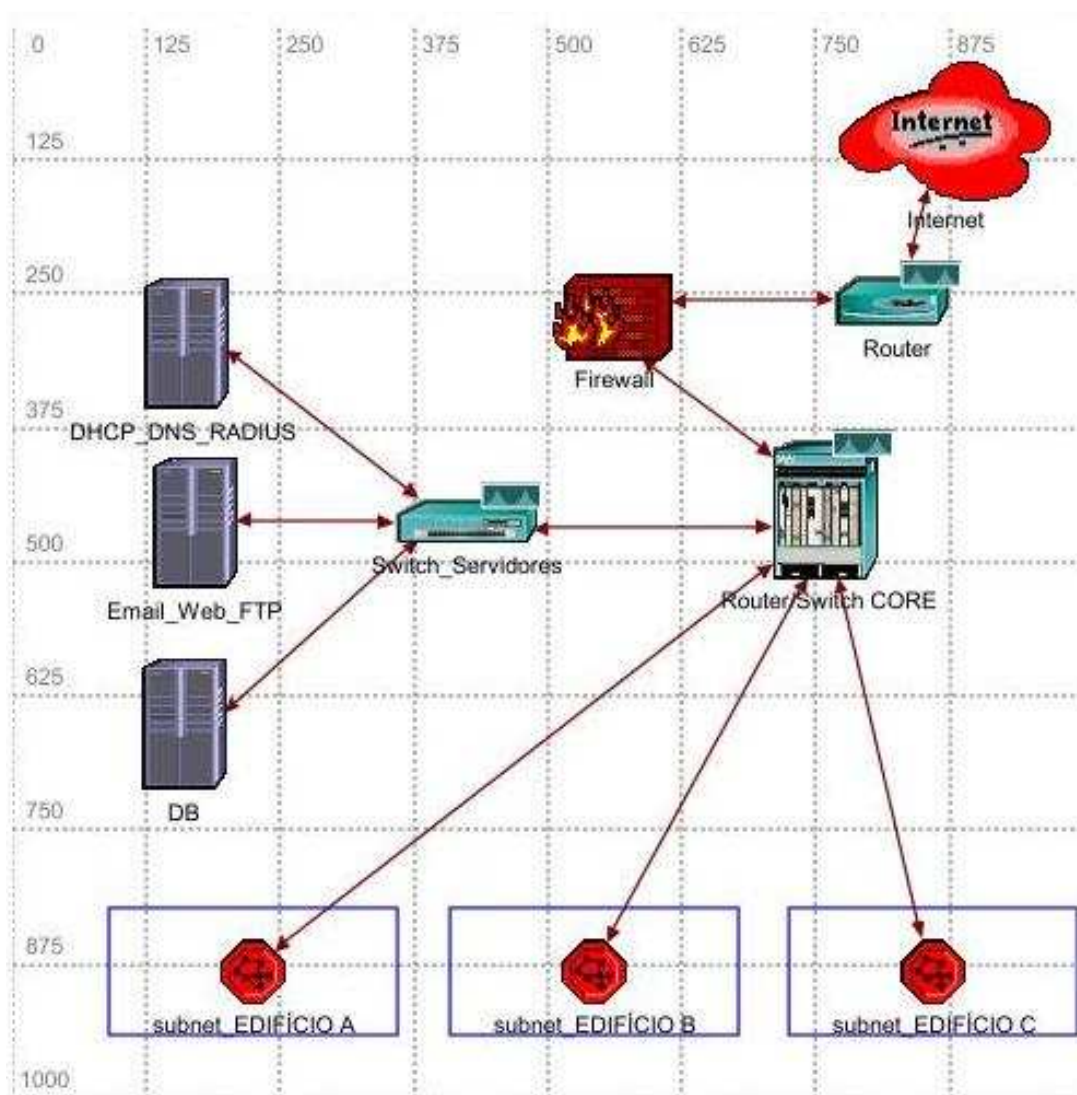


Figura 15. - Arquitectura Lógica da Rede

Podem ser visualizadas nas Figuras 16, 17 e 18 as estruturas das subredes de forma mais detalhada. A Figura 16 apresenta o detalhe da subrede do edifício A, a Figura 17 apresenta o detalhe da subrede do edifício B e a Figura 18 mostra o detalhe da subrede do edifício C.

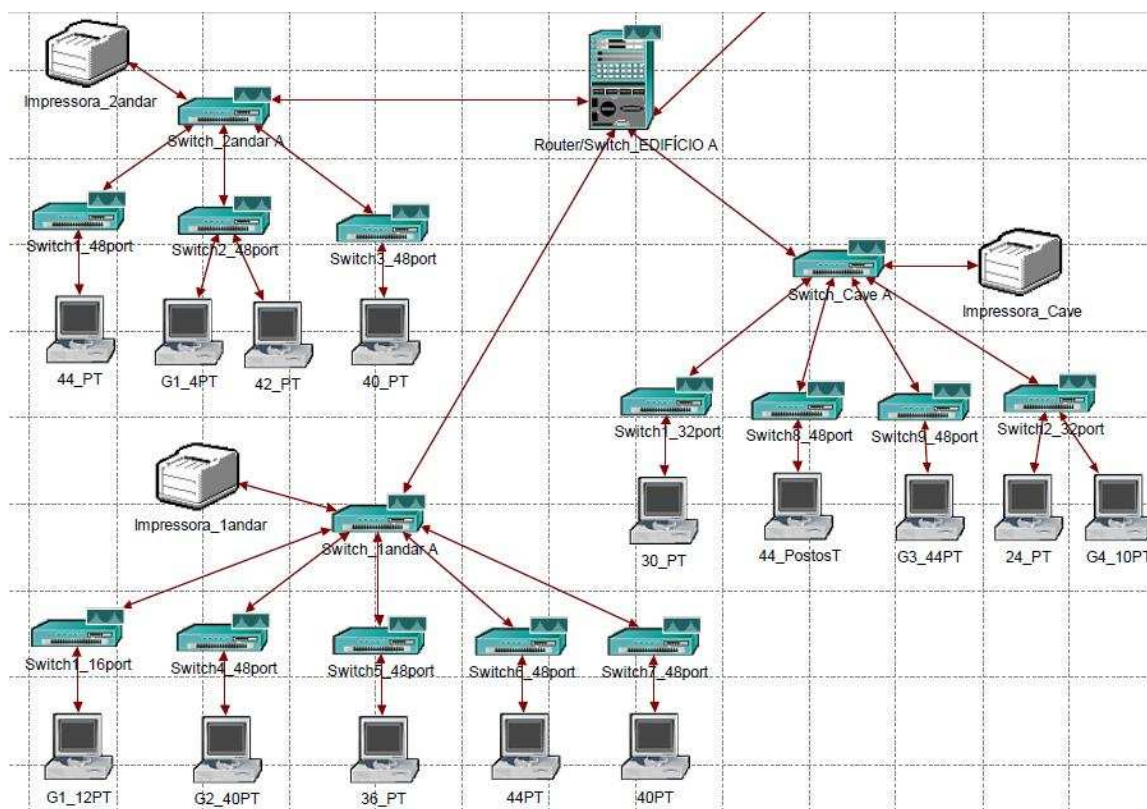


Figura 16. – Subrede do Edifício A

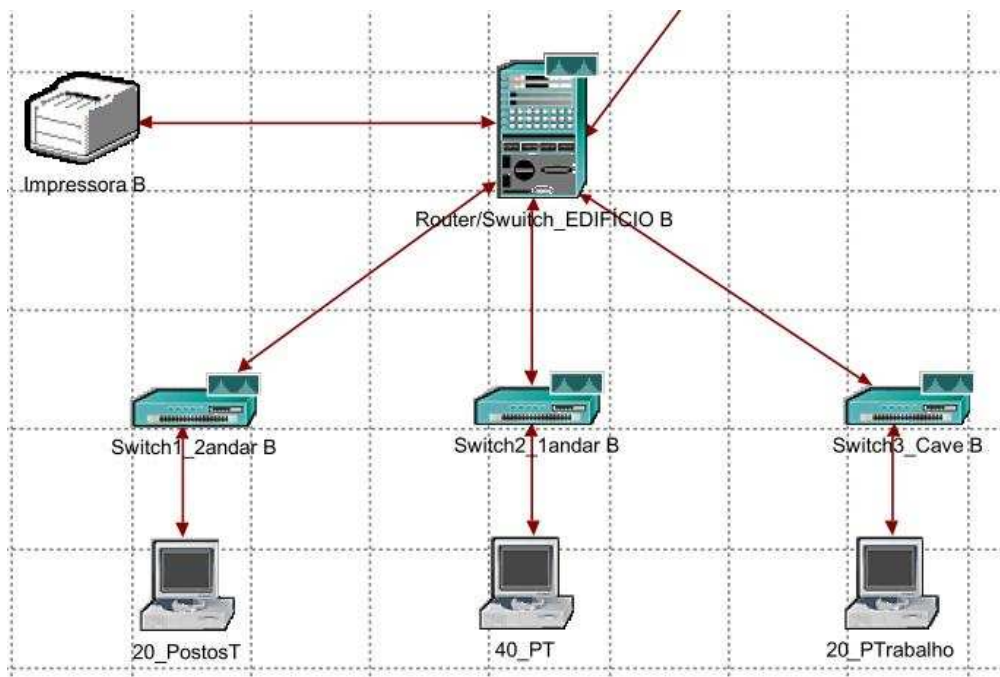


Figura 17. – Subrede do Edifício B

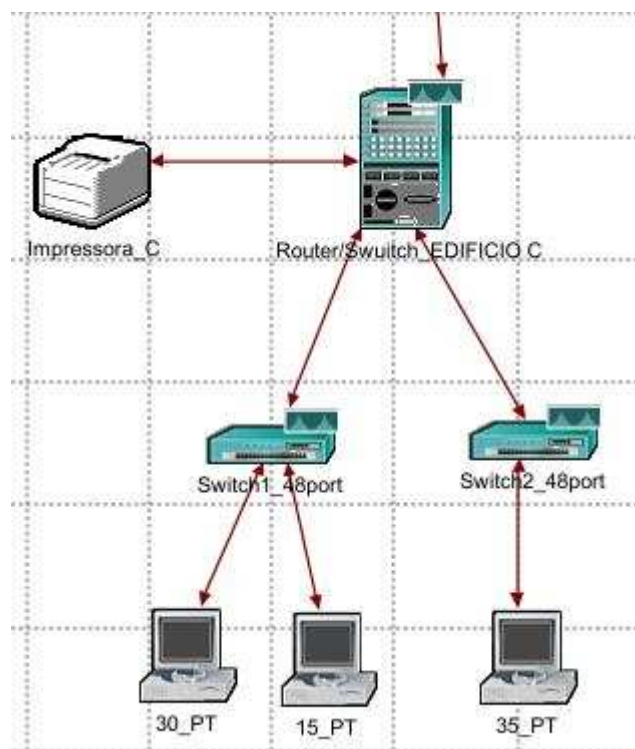


Figura 18. – Subrede do Edifício C

Como foi dito anteriormente, é necessário assegurar a redundância na topologia. Quer redundância a nível de servidores, router e switches quer ao nível das ligações. A Figura 19 apresenta a redundância física aplicada a rede. Como o servidor e o router/switch CORE são elementos críticos da rede, para além da redundância física em termos de ligação foi feita redundância em termos de equipamentos. Nos routers/switches e switches das subredes de cada edifício a redundância será feita apenas a nível de cablagem.

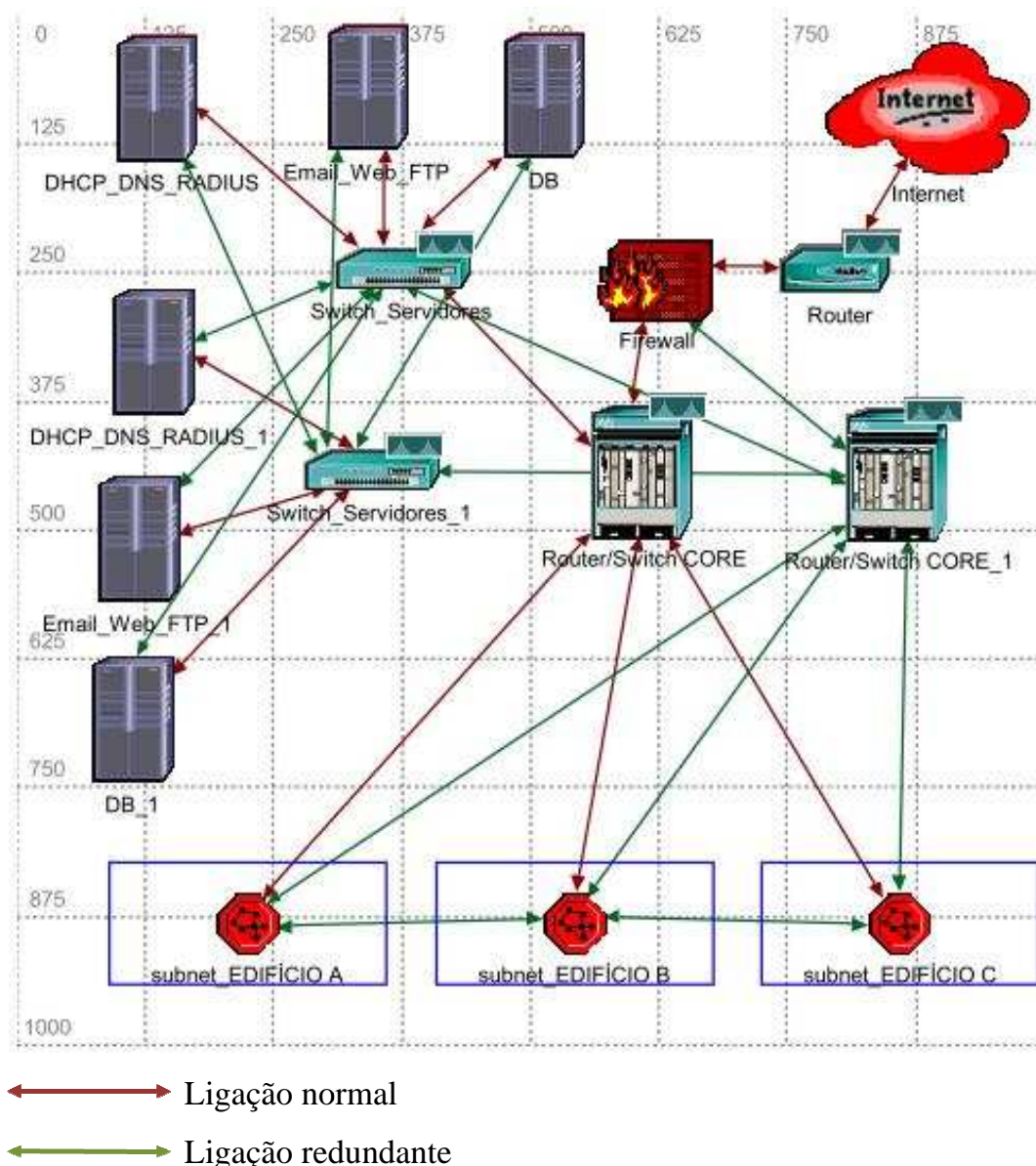


Figura 19. – Arquitectura Lógica com Redundância da Rede

Para se obter redundância lógica é necessário que os routers e switches tenham como características funcionais o suporte de protocolos de *routing* e STP respectivamente. Em funcionamento normal as ligações de redundância são logicamente desligadas e, em caso de falha, este protocolo activará as ligações necessárias para o funcionamento normal da rede, sem afectar a disponibilidade

da mesma. Para além dos servidores normais é necessário ter um ou mais servidores de *backup* (cópia do disco do servidor central). No caso de o servidor falhar pode ser removido e colocado outro em funcionamento.

3.4.1 VLAN

Havendo necessidade de separação de tráfego, teve-se em conta a aplicação de redes locais virtuais. Com a utilização de VLAN, é possível a definição de vários grupos de utilizadores e/ou servidores que comuniquem exclusivamente entre si, constituindo redes virtuais distintas sobre a mesma infra-estrutura física.

Quando se criam VLAN num switch, estão-se a criar várias redes, uma por VLAN, cada uma com o seu domínio de broadcast. Diferentes portas do switch podem pertencer a redes diferentes. Assim, com um único switch podemos criar vários domínios de *broadcast*. São criadas várias VLAN de acordo com o perfil dos utilizadores da rede, como indicado na Tabela 16. Como pode ser observado na Tabela 16, para além da criação das VLAN por perfil de utilizadores é criada uma VLAN para o administrador da rede na instituição. Também é criada uma VLAN para o VoIP e VCoIP, mesmo tendo em conta que nem todos os dispositivos que usem esta rede sejam membros dela.

Tabela 16. – Identificação das VLANs

VLAN	Descrição	Gama de endereços	Nº de bits da Mascara
Admin	Administração da Rede	120	/25
Server	Servidores	8	/28
PD	Presidência e Direcção	16	/27
FuncCF	Funcionários da Contabilidade e Finanças	40	/26
FunSG	Funcionários da Secretária Geral	44	/26
FunPr	Funcionários do Património	10	/28
FunAd	Funcionários Administrativos restantes	254	/24
Docs	Docentes	150	/24
Estuda	Estudantes	100	/25
VoIP	Voz sobre IP	254	/24
VCoIP	Videoconferência sobre IP	20	/27

Para abranger todos os potenciais utilizadores desta estrutura de rede é necessário que se atribua às VLAN endereços com máscaras de comprimento variável como especificadas na Tabela 16.

Utilizando mecanismos de tradução de endereços e portas, como NAT/PAT (Port Address Translation), permitirá que os dispositivos com endereços IP privados comuniquem com o exterior, a Internet. Sendo assim, estimando que 10% dos dispositivos da rede interna queiram aceder simultaneamente à Internet, incluindo os acessos a serviços controlados por proxies, e a mais do que um serviço (sem considerar a pretensão que eventuais servidores internos disponibilizem serviços para o exterior), será recomendável que para o

mecanismo do NAT esteja reservada uma rede com endereços IP públicos com uma gama de endereços mínima de 6 endereços, ou seja, uma máscara de 29 bit.

3.5 Especificações dos Equipamentos

3.5.1 Cablagem

De modo a obter um total aproveitamento do equipamento activo, é importante o projecto de um sistema de cablagem estruturado, flexível e genérico mas que ao mesmo tempo possua características de continuidade permitindo com isso manter o cabo mesmo que fosse necessário mudar o equipamento.

Para isso o mais conveniente será optar-se por uma instalação blindada de tomadas, painéis e cablagem UTP de acordo com as normas internacionais, para interligação dos bastidores com os postos de trabalho, nomeadamente cabos de Categoria 5 e com largura de banda de 100Mbit/s, o que possibilita comunicações até 1Gbit/s. Deverão ser suportadas as tecnologias actualmente mais divulgadas a nível de rede local (Ethernet, Fast Ethernet, Gigabit Ethernet). Nos postos de trabalho dever-se-á usar tecnologia Ethernet, na variante 10/100Base-TX (até 100Mbit/s).

A rede deverá ter 5 bastidores, dois dos quais recomendamos ser de 42U's e os restantes de 19U's. Nestes bastidores deverão existir painéis passivos para tomadas UTP (ISO 8877), destinados às ligações de cabo UTP, referentes às ligações de acesso e também painéis passivos para fibra óptica. Deve-se também

colocar um guia de *patching* entre cada dois painéis de tomadas e entre os painéis e o equipamento activo.

Na interligação entre bastidores de edifício, deverá ser usada fibra óptica multimodo de 50µm com suporte para Ethernet, devido às distâncias que o cabo tem de percorrer para efectuar a ligação. Actualmente a interligação entre os 3 bastidores [A, B e C] existentes já é feita por fibra óptica, esticada por via aérea. Neste projecto propomos a interligação por fibra óptica enterrada pois garante não só maior segurança como também maior fiabilidade da fibra óptica.

A rede a ser instalada deverá ter a capacidade de interligação de voz na cablagem (telefones, fax e modems) e a possibilidade de afectar dinamicamente qualquer tomada a serviços de voz ou de dados. Assim deixa de ser necessária a instalação de uma rede própria para a comunicação de voz, o que resulta em benefícios em termos de custos de infra-estrutura, flexibilidade e estética.

3.5.2 Equipamentos Activos

De um modo geral, os equipamentos activos a instalar deverão estar de acordo com as normas internacionais, sendo preferencialmente do tipo modulares, permitindo assim a regeneração destes equipamentos com o evoluir das necessidades e das tecnologias. Deverão suportar o protocolo TCP/IP para o acesso à Internet. Também deverão suportar fontes de alimentação redundantes. Por uma questão de segurança da rede estes equipamentos devem ter limitado o acesso ao serviço de "login" remoto e de preferência somente com sessões seguras, para tarefas de manutenção e configuração deverão permitir a restrição a

apenas acesso local a estes equipamentos. Como equipamentos activos temos os routers, switches e router/switch. Estes equipamentos são especificados a baixo.

Especificação do Router

Este router é o que fará a comunicação entre a rede interna e o exterior. Deverá suportar a família do protocolo TCP/IP, bem como as tecnologias Ethernet, PPP, ADSL e série síncrona. A nível da rede deverá suportar a família dos protocolos TCP/IP; também deverá ter suporte dos protocolos de *routing* RIP (*Routing Information Protocol*) e OSPF (*Open Shortest Path First*). No caso de futuramente a instituição pretender interligar-se a mais que um ISP (Internet Service Provider), será recomendável que este router também suporte o protocolo de *routing* exterior BGP (*Border Gateway Protocol*). Deverá ter suportar o protocolo SNMP para Gestão. Este router deverá estar equipado para montagem em bastidor de 19” e possibilitar gestão através de consola.

Especificação do Firewall

A firewall deverá estar colocada entre o router de acesso ao exterior e o router/switch CORE. Esta firewall para além das funções básicas de controlo de acesso deverá suportar serviços de *proxy* para minimizar a largura de banda. Esta terá de ser implementada com serviços de NAT/PAT de modo a permitir que os endereços dos dispositivos internos e suas respectivas portas sejam traduzidos num único endereço externo.

Especificação do Router/Switch CORE

O router/switch CORE é um switch de nível 2/3 que faz *routing*. Este fará o controlo do tráfego da rede interna. Deverá suportar filtragem dinâmica das

portas dos protocolos TCP e UDP. Terá 1 porta 100Base-T para ligação a firewall e 8 portas 1000Base-SX para ligação aos routers/switch de cada edifício. Terá que ter capacidade de funcionar como servidor DHCP para a rede interna e suporte do protocolo SNMP para Gestão. Este também deverá ter possibilidade de gestão através de consola e de montagem em bastidor de 19”.

Especificação do Router/Switch

O router/switch também é um switch de nível 2/3 que estará colocado em cada um dos três edifícios da instituição. Deverá suportar funções de controlo de acesso e de autenticação de utilizadores, sendo implementado com protocolos de segurança CHAP (Challenge Handshake Authentication Protocol) e PAP (Password Authentication Protocol), completado com mecanismos de segurança do tipo "*access lists*" ou filtros. Também deverá ter Integração de voz, vídeo e dados. Deverá ter 2 portas 1000Base-SX, uma para ligação ao router/switch CORE e outra para ligação redundante ao router/switch de outro edifício, bem como ter interfaces Ethernet de 10/100/1000Mbit/s para ligar os switches locais. Deverá ser configurado com o protocolo STP, possibilitar gestão através da consola e ser equipado para montagem em bastidor de 19”.

Especificação do Switch

Este é um switch local de nível 2 com interfaces Ethernet de 10/100/1000Mbit/s e configurado com protocolo STP. Este deverá ser equipado para montagem em bastidor de 19” e possibilitar gestão através de consola.

3.5.3 Equipamentos de Gestão e Segurança

Hoje em dia cada vez mais as redes necessitam de ter implementados serviços gestão e segurança. Mesmo em redes de pequena dimensão, torna-se indispensável a utilização de ferramentas de gestão e de segurança. A gestão de redes consiste na monitorização da operacionalidade dos recursos da rede com o objectivo de determinar possíveis falhas e problemas, bem como ajustar a arquitectura e as configurações dos dispositivos com base nos dados recolhidos no monitoramento, para optimizar a utilização da rede. A segurança de redes procura minimizar os problemas associados ao acesso não autorizado a recursos da rede.

3.5.4 Bastidores

Todos os bastidores devem estar equipados com unidades UPS para garantirem o funcionamento normal da rede em caso de falha de energia eléctrica (problema local frequente) até o início de funcionamento do gerador, ou outra fonte alternativa de energia eléctrica, da Instituição. Em todas as salas onde se irão instalar os bastidores, como indica a Figura 20, deverá haver um sistema de ar condicionado, e cada bastidor deverá conter um kit de ventilação para remover o ar quente gerado pelos equipamentos.

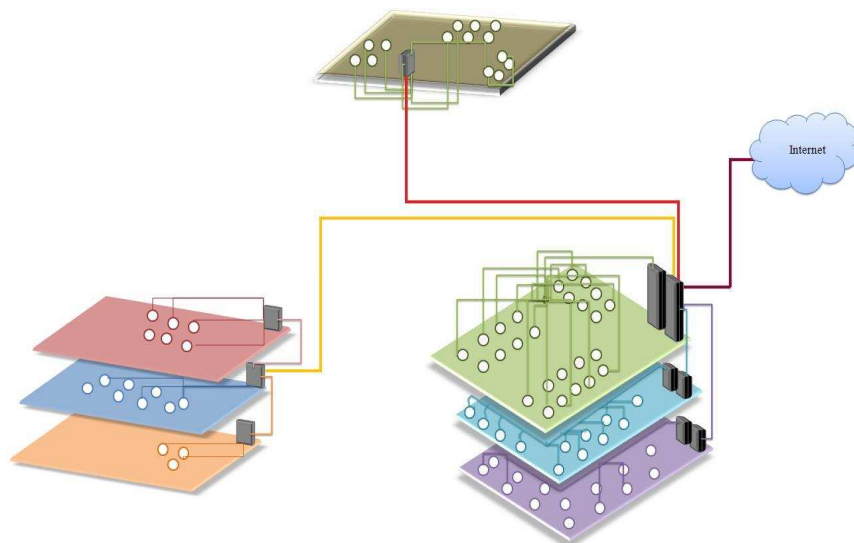


Figura 20. – Localização dos Bastidores em cada Edifício

O bastidor principal deverá albergar todo o equipamento associado à rede local, bem como o equipamento destinado às comunicações com o exterior. Os bastidores espalhados pelos pisos dos três edifícios irão albergar todo o equipamento da subrede correspondente ao piso em causa. Os bastidores a instalar terão especificações de acordo às normas IEC 297, DIN 41494 e EIA RS310C. A Figura 21 mostra como podem ser os bastidores *rack* de 19”



Figura 21. – Exemplos de Bastidores *rack* de 19"

3.6 Resumo

Neste capítulo, numa primeira fase, fez-se o levantamento dos requisitos dos utilizadores, aplicações, dispositivos e rede. Depois deste, fez-se uma descrição da topologia da rede na instituição. Na fase seguinte dimensionaram-se os fluxos e os débitos das ligações para esta estrutura da rede. Tendo o dimensionamento das ligações foi possível fazer a especificação dos equipamentos necessários para a implementação da estrutura da rede e, na fase final, apresentar a arquitectura lógica da rede para o ISCED.

4 Conclusões e Trabalho Futuro

Espera-se que a implementação e utilização da rede no ISCED traga benefícios à instituição. Desses benefícios destacam-se o acesso à Internet de forma livre, pontos de acesso à rede para os computadores, mais postos de trabalho para os estudantes do que os existentes actualmente e ligação à rede dos computadores das duas salas do laboratório do Curso de Informática. Esta estrutura de rede poderá ser também usada numa futura plataforma de *e-learning* para ensino à distância.

Esta dissertação teve como principal objectivo planear e projectar a rede de comunicações do ISCED. Os resultados mais importantes deste projecto são os seguintes:

1. Levantamento de requisitos de comunicação do ISCED. Foram analisados os tipos de utilizadores do ISCED e os serviços que estes necessitavam da rede. Concluiu-se que o ISCED era formado por sete grupos de utilizadores e que todos tinham necessidades comuns de serviços de email, Web e partilha de ficheiros. Alguns destes grupos tinham necessidade de serviços/aplicações específicas, tais como aplicações de gestão financeira, de pessoal, de stock e de estudantes.
2. Planeamento da rede. Foi estimado o tipo de tráfego que passará pela rede, dimensionaram-se as ligações e fez-se um projecto preliminar da rede. Com base neste planeamento foi possível determinar os tipos de equipamento a utilizar.

No decurso deste projecto foram encontradas algumas dificuldades das quais se destaca a falta de meios adequados para cálculos e medições, o que levou a conceber a rede com base em estimativas da quantidade de tráfego

Uma vez que o edifício principal e o edifício do lar do ISCED são muito antigos temos que ser cuidadosos na instalação da cablagem. A fibra óptica usada para interligar os edifícios deverá ser enterrada. É também necessário referir que a instalação dos bastidores, cabos e tomadas, deverá ser feita de acordo com as normas de cablagem e as boas práticas de instalação.

4.1.1 Trabalho Futuro

O trabalho futuro consiste em implementar uma rede em malha sem fios (*Wireless Mesh Network* – WMN), de modo a proporcionar cobertura Wi-Fi em todo o ISCED de maneira fiável e económica. Com uma rede WMN, o ISCED poderá estender os seus serviços e aplicações orientados para rede com fios para além das paredes dos seus edifícios.

5 Bibliografia

- [1] James D. McCabe. Network Analysis, Architecture, and Design, 3rd Ed., by ELSEVIER, www.elsevier.com , 2007

- [2] Edmundo Monteiro & Fernando Boavida. Engenharia de Redes Informáticas, 8ª Edição. Editora FCA, Agosto 2000.
Edmundo Monteiro – <http://www.dei.uc.pt/~edmundo>,
Fernando Boavida – <http://www.dei.uc.pt/~boavida>

- [3] Lindeberg Barros de Sousa. Projectos e Implementação de Redes; Fundamentos, Arquitecturas, Soluções e Planeamento. Editora Érica, 2007.
www.editoraerica.com.br

- [4] José Gouveia & Alberto Magalhães. Redes de Computadores, curso completo, 4ªedição. Editora FCA, Julho 2005. www.fca.pt

- [5] Larry L. Peterson & Bruce S. Davie. Redes de Computadores, uma abordagem Sistémica, 2ª edição. Editora LTC, 2004. www.ltceditora.com.br

- [6] Mário Véstias. Redes CISCO para profissionais, 4ª Edição. Editora FCA, Abril 2009

- [7] Paulo Loureiro. TCP/IP em redes Microsoft para Profissionais, 5ª Edição.

- [8] Pedro Fernandes Moral. Trabalho Final, Projecto de Redes, Instituto Politécnico de Tomar – Escola Superior de Tecnologia de Tomar, Departamento de Engenharia Informática, 2007

- [9] Guilherme Silva Vilela. Caracterização de Tráfego utilizando Classificação de Fluxos de Comunicação. Engenharia de Sistemas e Computadores – Universidade Federal do Rio de Janeiro, 2006.
www.ravel.ufrj.br/arquivosPublicacoes/monografia_cos871_vilela.pdf
- [10] João Neves. Artigo de Análise de Fluxos. Faculdade de Engenharia da Universidade do Porto, 2007.
www.inescporto.pt/~jneves/feup/2008-2009/pars/fluxos.pdf
- [11] Rafael Gomes Machado. Sistema de Informação Baseado numa Intranet para a Gestão Pedagógica de uma Escola do Ensino Secundário. Faculdade de Engenharia da Universidade do Porto, Departamento de Engenharia Electrotécnica e de Computadores, 1999
- [12] Packet Tracer. Ferramenta de simulação de redes de comunicações desenvolvido pela CISCO.
www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html
- [13] OPNET IT Guru. Ferramenta de simulação de redes desenvolvida pela OPNET Technologies. www.opnet.com

6 Anexos

Anexo A – Plantas

O edifício principal é composto por 3 pisos: Cave, 1º andar e 2º andar. O servidor de comunicações já existente encontra-se no 2º andar. Para este projecto está-se a propor um bastidor para cada andar.

No edifício principal, o bastidor existente no 2º andar será designado por A2 e encontra-se situado na sala indicada na Figura 22. Encontrar-se-á aqui a ligação CORE da instituição. O 1º andar terá o bastidor A1, dará cobertura para todo o piso e estará situado na sala indicada na Figura 23. Na cave (é uma cave a nível do chão) o bastidor será designado por AC e dará cobertura a todo esse piso. Este bastidor estará situado na sala como se pode ver na Figura 24.

As Figuras 25 e 26 apresentam as plantas do 2º e 1º andar do edifício do Lar. Pode ser observado que o bastidor principal do edifício do Lar encontra-se no 1º andar e designado por B e encontra-se localizado na sala indicada na Figura 26.

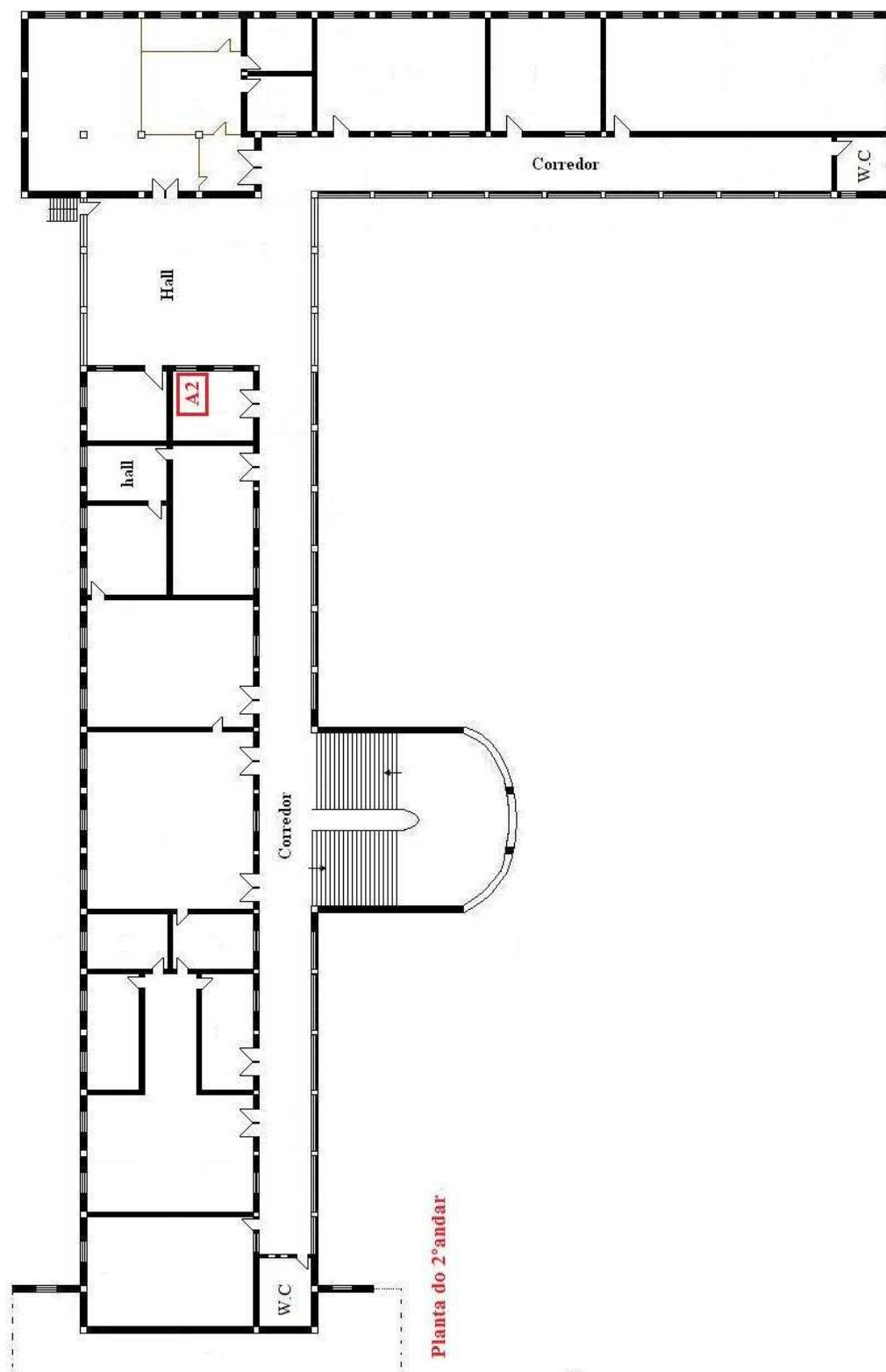


Figura 22. – Planta do 2º Andar do Edifício Principal

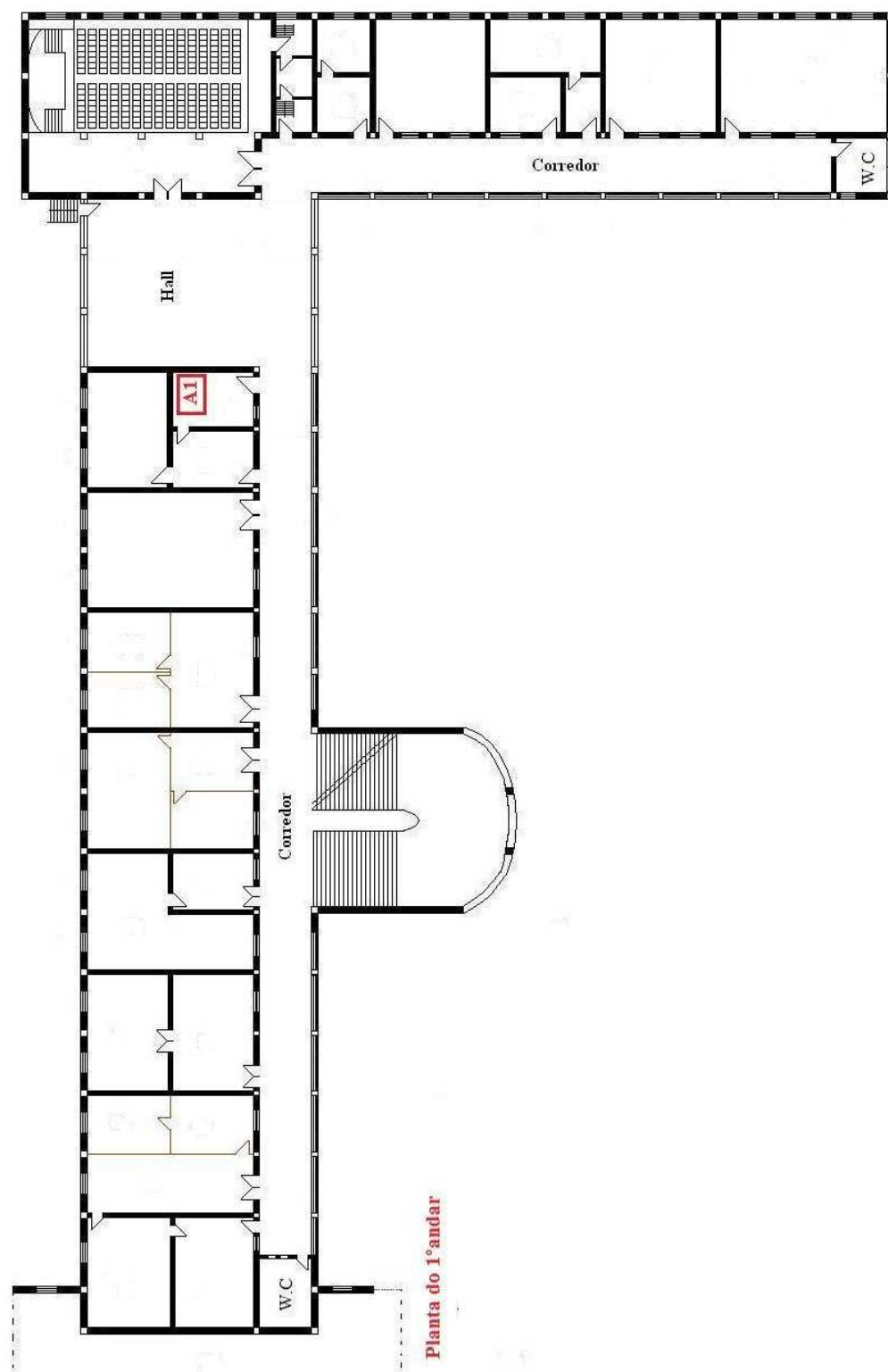


Figura 23. – Planta do 1º Andar do Edifício Principal

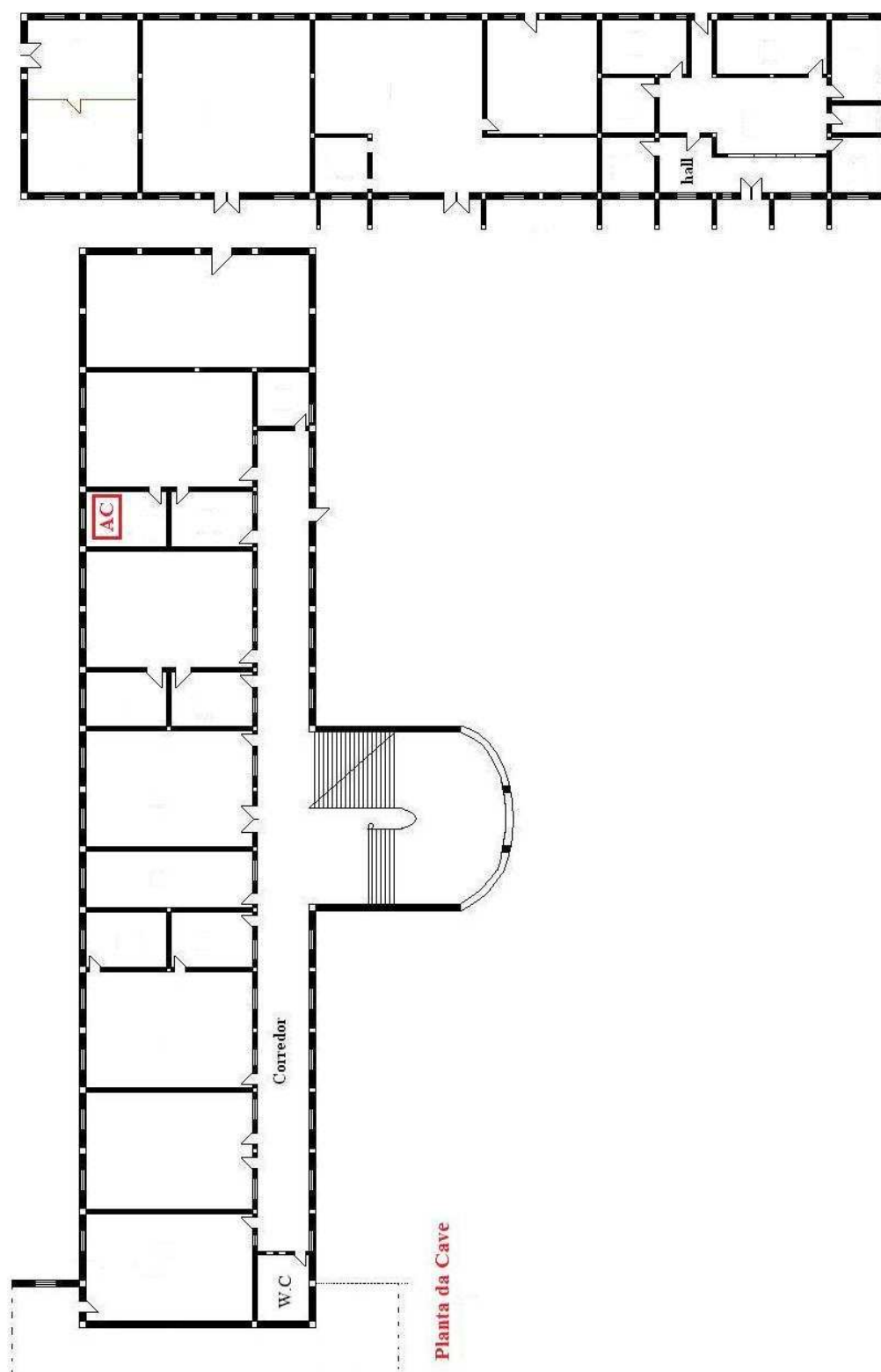


Figura 24. – Planta da Cave do Edifício Principal

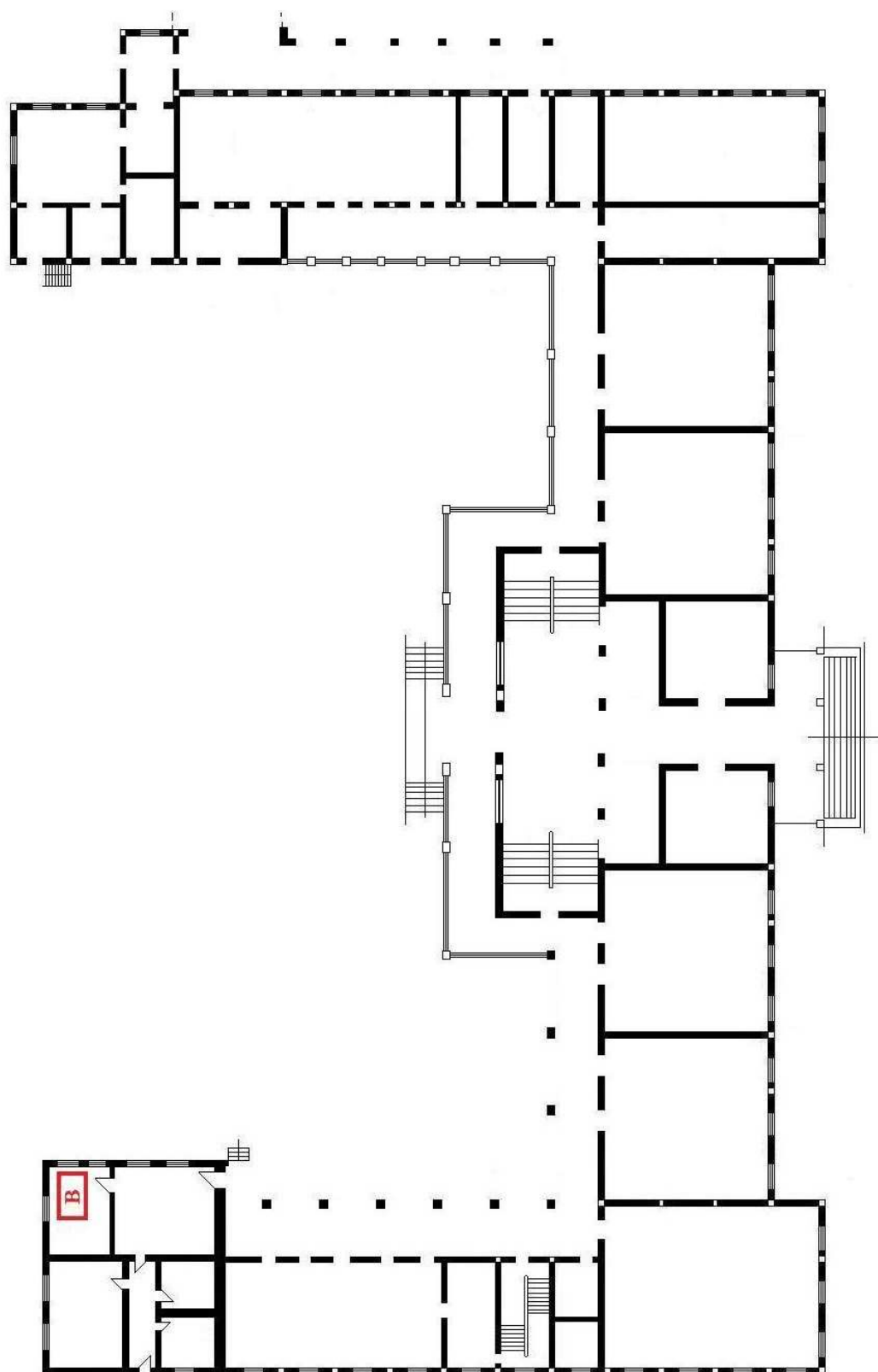


Figura 25. – Planta do 2º Andar do Edifício do Lar

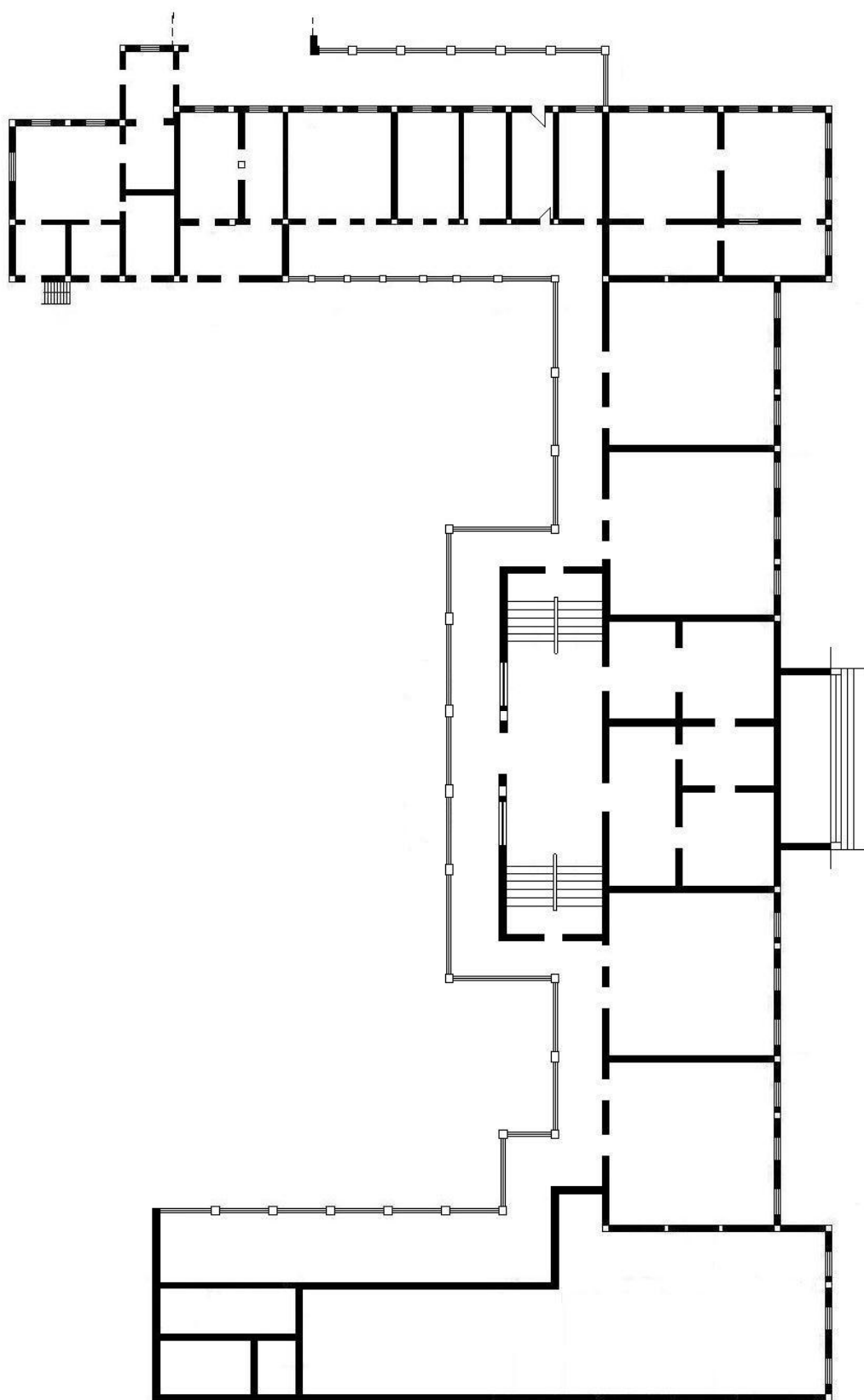
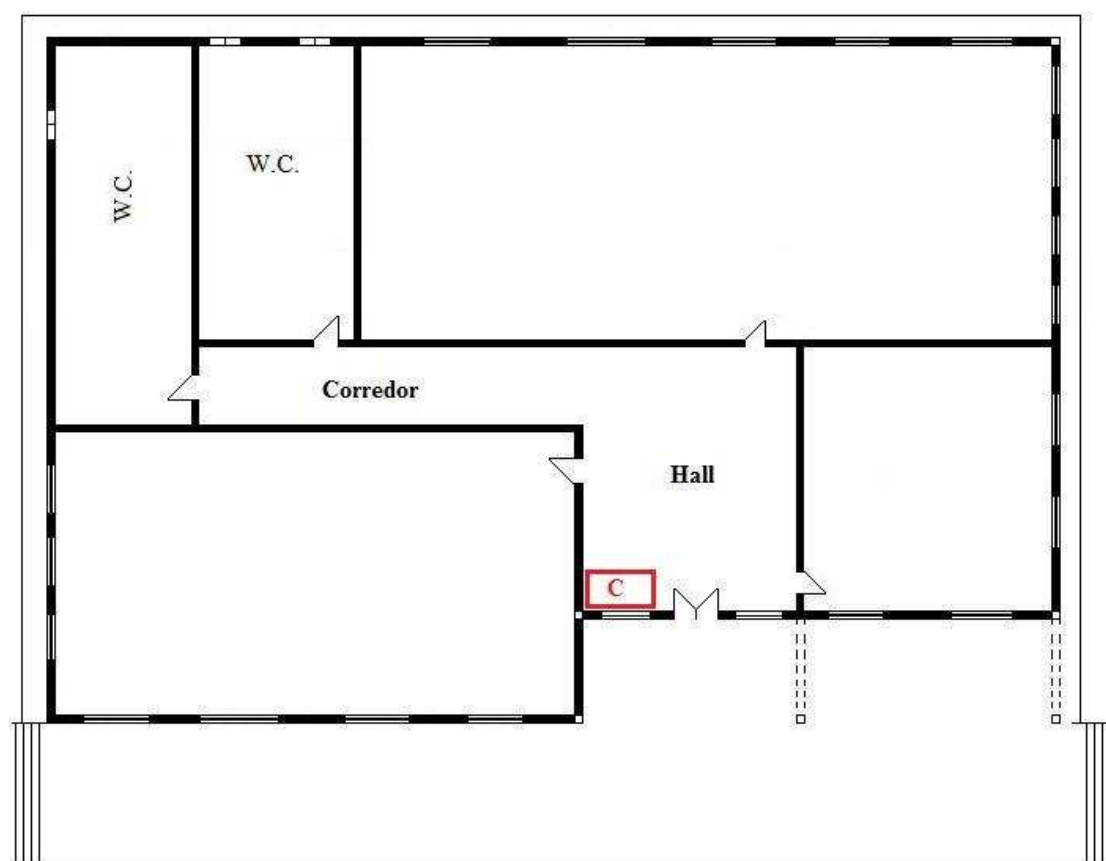


Figura 26. – Planta do 1º Andar do Edifício do Lar

O laboratório de informática é composto por duas salas de informática com um total de 65 computadores. Para a implementação da nova rede iremos aproveitar toda a estrutura de cablagem já existente, alterando apenas o equipamento activo no bastidor C, como se pode ver na Figura 27.



Planta do Laboratório de Informática

Figura 27. – Planta do Laboratório de Informática

Anexo B – Medições

Tabela 17. – Quantidades de Equipamentos Passivos

Equipamento Passivo				
Componente	QT por Edifício			Total
	A	B	C	
Adaptador ST	1	1	1	3
Bastidor de 19", 19U	2	1	1	4
Bastidor de 19", 42U	1	0	0	1
Cabo UTP CAT 5e	500	100	100	700
Cabo de fibra óptica de 8 fibras	8	2	2	12
Calha plástica (100x50) com acessórios	140	90	70	300
Chicote fibra óptica duplo ST-ST, de 2m	50	10	10	70
Chicotes UTP CAT 5 de 3m	50	50	50	150
Chicotes UTP CAT 5 de 15m	50	30	30	110
Conector de fibra óptica ST	32	16	16	64
Conectores RJ-45	1000	200	200	1400
Guias de cabos	22	5	5	32
Kit de rodas	1	1	1	3
Kit de ventilação	1	1	1	3
Painel ISO 8877 com 32 posições, blindado	10	0	0	10
Painel ISO 8877 com 48 posições, blindado	9	2	2	13
Painel para fibra óptica com 12 posições	1	1	1	3
Réguas de tomadas eléctricas	2	1	1	4
Tomadas ISO 8877 CAT 5 dupla	200	25	20	245
Tomadas ISO 8877 CAT 5 simples	50	50	60	160

Tabela 18. – Quantidades de Equipamentos Activos

Equipamento Activo, Dispositivos e Ferramentas				
Componente	QT por Edifício			Total
	A	B	C	
Alicate de cravamento RJ-45/RJ-11	1	1	1	3
Ferramenta de cravamento tomadas e painéis	1	1	1	3
Firewall	1	0	0	1
Impressora, Scanner	3	1	2	6
Router IP	1	0	0	1
Router/Switch CORE, 2x10/100/100B-Tx + 8x10/100/1000B-SX	1	0	0	1
Router/Switch, 8x10/100/1000B-TX + 2x10/100/1000B-SX	1	1	1	3
Servidor BD	1	0	0	1
Servidor DHCP, DNS, RADIUS	1	0	0	1
Servidor Email, Web, FTP	1	0	0	1
Switch 16x10/100/1000B-TX	5	0	0	5
Switch 24x10/100/1000B-TX	0	2	0	2
Switch 32x10/100/1000B-TX	2	0	0	2
Switch 48x10/100/1000B-TX	9	1	2	12
UPS 1000 vas, rack-mountable	3	1	1	5
UPS 8000 vas, rack-mountable	1	0	0	1

Anexo C – Orçamento

Os custos apresentados na Tabela 42 foram estimados a partir dos valores do mercado actuais.

Tabela 19. – Orçamento do Equipamento Passivo

Custos do Equipamento Passivo			
Componente	QT	Custo Unitário	Custo Total[€]
Adaptador ST	3	5,00	15,00
Bastidor de 19", 19U	4	700,00	2.800,00
Bastidor de 19", 42U	1	1.700,00	1.700,00
Cabo de fibra óptica de 8 fibras	700	140,00	98.000,00
Cabo UTP CAT 5e	12	65,00	780,00
Calha plástica (100x50) com acessórios	300	7,00	2.100,00
Chicote fibra óptica duplo ST-ST, de 2m	70	20,00	1.400,00
Chicotes UTP CAT 5 de 3m	150	3,00	450,00
Chicotes UTP CAT 5 de 15m	110	7,00	770,00
Conector de fibra óptica ST	64	80,00	5.120,00
Conectores RJ-45	1400	4,00	5.600,00
Guias de cabos	32	290,00	9.280,00
Kit de rodas	3	60,00	180,00
Kit de ventilação	3	47,00	141,00
Painel ISO 8877 com 32 posições, blindado	10	200,00	2.000,00
Painel ISO 8877 com 48 posições, blindado	13	280,00	3.640,00
Painel para fibra óptica com 12 posições	3	110,00	330,00
Réguas de tomadas eléctricas	4	86,00	344,00
Tomadas ISO 8877 CAT 5 dupla	245	10,00	2.450,00
Tomadas ISO 8877 CAT 5 simples	160	10,00	1.600,00
TOTAL			138.700,00

Tabela 20. – Orçamento Equipamento Activo

Custo dos Equipamento Activo, dispositivos e Ferramentas			
Componente	QT	Custo Unitário	Custo Total[€]
Alicate de cravamento RJ-45/RJ-11	3	35,00	105,00
Ferramenta de cravamento tomadas e painéis	3	60,00	180,00
Firewall	1	60,00	60,00
Impressora, Scanner	6	190,00	1.140,00
Router IP	1	95,00	95,00
Router/Switch CORE, 2x10/100/1000B-Tx + 8x10/100/1000B-SX	1	3.300,00	3.300,00
Router/Switch, 8x10/100/1000B-TX + 2x10/100/1000B-SX	3	2.800,00	8.400,00
Servidor BD	1	300,00	300,00
Servidor DHCP, DNS, RADIUS	1	150,00	150,00
Servidor Email, Web, FTP	1	350,00	350,00
Switch 16x10/100/1000B-TX	5	85,00	425,00
Switch 24x10/100/1000B-TX	2	220,00	440,00
Switch 32x10/100/1000B-TX	2	290,00	580,00
Switch 48x10/100/1000B-TX	12	500,00	6.000,00
UPS 1000 VA, rack-mountable	5	55,00	275,00
UPS 8000 VA, rack-mountable	1	4.700,00	4.700,00
TOTAL			26.500,00

O custo de aquisição da rede é de **165.200.00€**. O custo de exploração e manutenção da rede tem um acréscimo na ordem dos 15% a 20%. No custo de exploração tem-se em conta o custo do aluguer do circuito para o acesso à Internet. O custo do circuito a alugar para o acesso à Internet irá depender do novo contrato estabelecido entre o ISCED e um operador em Angola